SAFEBOOK 3

Sistemi di controllo legati alla sicurezza delle macchine

Principi, standard e implementazione

Sommario

Allen-Bradley

Legislazione e direttive UE

Obiettivo di questa sezione è fornire una guida per tutti coloro che si occupano di sicurezza delle macchine e, in particolare, dei sistemi di protezione all'interno dell'Unione Europea. Ed è rivolta sia ai progettisti che agli utilizzatori di apparecchiature industriali.

Per promuovere il concetto di mercato aperto nell'Area Economica Europea (EEA) (comprendente gli stati membri UE e altri 3 paesi), tutti gli stati membri sono tenuti ad adottare una legislazione che definisca i requisiti di sicurezza fondamentali per le macchine e il loro uso.

Le macchine che non soddisfano tali requisiti non possono essere commercializzate all'interno dei paesi EEA.

Esistono diverse direttive europee applicabili alla sicurezza delle apparecchiature e delle macchine industriali ma le due più importanti sono le seguenti:

1 La Direttiva Macchine

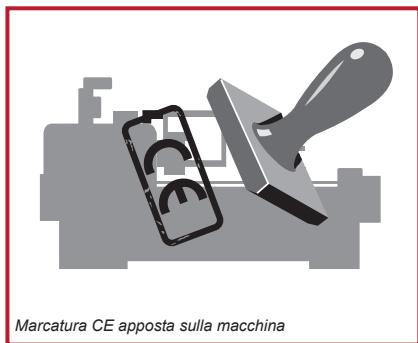
2 La Direttiva relativa ai requisiti minimi di sicurezza e di salute per l'uso delle attrezzature di lavoro da parte dei lavoratori durante il lavoro

Queste due direttive sono direttamente correlate e i requisiti essenziali per la salute e la sicurezza (EHSR) previsti dalla Direttiva Macchine possono essere utilizzati per confermare la sicurezza delle attrezzature descritta nella direttiva sull'uso delle attrezzature di lavoro.

Questa sezione descrive alcuni aspetti di entrambe le direttive. Chi si occupa di progettazione, fornitura, acquisto o utilizzo delle attrezzature industriali all'interno dei paesi SEE e di alcuni altri paesi europei dovrebbe prendere conoscenza dei requisiti previsti da tali testi. I fornitori e gli utilizzatori di macchine che non agiscono conformemente a tali direttive non potranno fornire o operare in questi paesi.

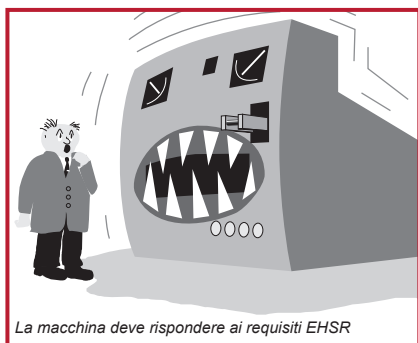
Esistono altre direttive europee relative alla sicurezza industriale. La maggior parte di queste è piuttosto specialistica nell'applicazione e, per questo motivo, tali testi non saranno trattati nella presente sezione; tuttavia, è importante notare che, laddove pertinente, i loro requisiti devono comunque essere rispettati, come nel caso della Direttiva Bassa Tensione e della Direttiva ATEX.

La Direttiva Macchine

Tale direttiva (98/37/EC) riguarda la fornitura di macchinari nuovi e di altre attrezzature, compresi i componenti di sicurezza. Fornire macchinari non conformi a questa Direttiva è un reato. Ciò significa che occorre soddisfare tutti i requisiti essenziali per la salute e la sicurezza (EHSR) elencati nell'Allegato I della direttiva, effettuare una adeguata valutazione di conformità, fornire una "Dichiarazione di conformità" e apporre la marcatura CE.

Marcatura CE apposta sulla macchina

Le principali disposizioni della direttiva sono entrate in vigore il 1° gennaio 1995 per le macchine e il 1° gennaio 1997 per i componenti di sicurezza. È stato previsto un periodo di transizione di due anni durante il quale era possibile scegliere se adottare i regolamenti nazionali esistenti o la nuova direttiva. Il produttore, l'importatore o l'utente finale hanno la responsabilità di garantire che le attrezzature fornite siano conformi alla direttiva.

Una nuova versione della Direttiva Macchine è stata pubblicata nel 2006, denominata 2006/42/EC. La nuova direttiva non sostituirà le disposizioni di quella precedente fino alla fine del 2009. Nel frattempo, la Direttiva Macchine esistente si applica in pieno. Il testo che segue tratta l'attuale Direttiva 98/37/EC ma è necessario considerare che, per molti tipi di macchine, le modifiche apportate alla nuova direttiva in termini di requisiti fondamentali sono soltanto di lieve entità.

Requisiti fondamentali di salute e sicurezza

La macchina deve rispondere ai requisiti EHSR

La direttiva fornisce un elenco dei requisiti fondamentali di salute e sicurezza (EHSR) a cui le macchine, dove pertinente, devono conformarsi. Scopo di questo elenco è quello di garantire che i macchinari siano sicuri, progettati e realizzati in modo che le operazioni di uso, regolazione e manutenzione non costituiscano un rischio per le persone, in tutte le fasi della loro vita operativa.

La direttiva fornisce inoltre una gerarchia delle misure atte a eliminare il rischio:

(1) Sicurezza intrinseca – Nei casi in cui è possibile, il progetto stesso deve evitare l'insorgere di qualsiasi pericolo.

Laddove non è possibile, occorre usare **(2) Dispositivi di protezione aggiuntivi** come, ad esempio, protezioni con punti di accesso interbloccati, protezioni non materiali quali barriere fotoelettriche, pedane sensibili, ecc.

Qualsiasi rischio residuo che non possa essere evitato con i metodi sopra elencati deve essere evitato tramite l'uso di **(3) Dispositivi di protezione e/o formazione del personale**. Il fornitore della macchina deve specificare quanto appropriato.

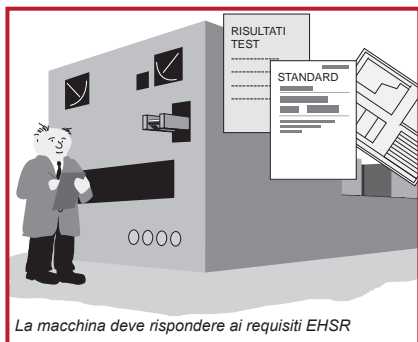
La macchina deve essere realizzata con materiali adatti alla costruzione e all'utilizzo. Devono inoltre essere fornite illuminazione e strumenti di manipolazione adeguate. I comandi e i sistemi di controllo devono essere sicuri e affidabili. Le macchine non devono essere in grado di avviarsi inaspettatamente e devono essere fornite di almeno un dispositivo di arresto di emergenza. Occorre prestare particolare attenzione alle installazioni complesse in cui i processi a monte o a valle possano influire sulla sicurezza della macchina. Un eventuale guasto all'alimentazione o ad un circuito di controllo non deve provocare situazioni pericolose. Le macchine devono essere stabili e in grado di resistere alle sollecitazioni prevedibili. Non devono presentare spigoli o superfici che possano causare ferite.

È necessario utilizzare protezioni o dispositivi di protezione che evitino l'insorgenza di rischi dovuti ad esempio a parti in movimento. Tali dispositivi devono essere robusti e difficili da escludere. Le protezioni fisse devono essere montate in modo che possano essere rimosse solo con l'ausilio di utensili. Le protezioni mobili devono essere interbloccate. Le protezioni regolabili non devono richiedere l'uso di utensili.

Occorre evitare l'insorgenza di rischi di natura elettrica o legati all'alimentazione. Il rischio di danni personali dovuti a temperatura, esplosione, rumore, vibrazione, polvere, gas o radiazioni deve essere minimo. Devono essere previste disposizioni appropriate per la manutenzione e la riparazione. Devono inoltre essere forniti dispositivi di indicazione e allarme sufficienti. I macchinari devono esser forniti completi delle istruzioni per un'installazione, uso, regolazione ecc. sicuri.

Valutazione di conformità

Il progettista o qualsiasi altro ente responsabile deve essere in grado di attestare la conformità ai requisiti essenziali di sicurezza e salute. Questo dossier dovrebbe includere tutte le informazioni pertinenti, come risultati dei test, schemi, specifiche, ecc.

La macchina deve rispondere ai requisiti EHSR

Una norma armonizzata europea (EN) pubblicata sulla Gazzetta Ufficiale dell'Unione Europea (OJ) sotto la Direttiva Macchine – la cui data di cessazione di presunzione di conformità non sia scaduta – conferisce presunzione di conformità a determinati requisiti EHSR (molte norme recenti pubblicate sulla Gazzetta includono un riferimento incrociato che identifica i requisiti EHSR coperti dalla norma).

Di conseguenza, quando le apparecchiature sono conformi alle attuali norme armonizzate europee, il compito di dimostrare la conformità con gli EHSR è molto semplificato e il costruttore beneficia anche della maggiore certezza legale. Tali standard non sono richiesti per legge ma il loro utilizzo è fortemente consigliato, poiché dimostrare la conformità tramite metodi alternativi può essere molto complesso. Tali norme supportano la Direttiva Macchine e sono prodotte dal CEN (European Committee for Standardization) in collaborazione con ISO e da CENELEC (European Committee for Electrotechnical Standardization) in collaborazione con l'IEC.

È necessario condurre una valutazione dei rischi approfondita e documentata per garantire che siano stati analizzati tutti i potenziali rischi della macchina. Inoltre, è responsabilità del costruttore assicurare il rispetto di tutti i requisiti EHSR, anche di quelli non trattati dalle norme armonizzate EN.

Dossier tecnico

La persona responsabile della dichiarazione di conformità deve garantire che la seguente documentazione sia disponibile ai fini di eventuali ispezioni.

Un dossier tecnico che comprende quanto segue.

1. I disegni generali dell'attrezzatura, compresi i disegni del circuito di controllo.

2. I disegni dettagliati, le note di calcolo ecc. richiesti per la verifica della conformità della macchina con i requisiti essenziali di sicurezza e salute.

3. Un elenco di quanto segue:
   - i requisiti essenziali di sicurezza e salute (EHSR) pertinenti all'attrezzatura
   - le norme europee armonizzate applicabili
   - altre norme applicabili
   - le specifiche tecniche di progettazione.

4. Una descrizione dei metodi adottati per eliminare i rischi presentati dalla macchina.

5. Se lo si desidera, eventuali relazioni o certificati tecnici ottenuti da un ente o un laboratorio certificatore.

6. Se viene dichiarata la conformità con una norma armonizzata europea, le relazioni tecniche contenenti i risultati dei relativi test.

7. Una copia delle istruzioni relative alla macchina.

Per la produzione in serie, i dettagli sulla misure interne (ad esempio, sistemi di qualità) usate per garantire che tutti i macchinari prodotti siano conformi.

- I produttori devono eseguire tutte le ricerche o i test necessari su componenti, accessori o macchine complete per determinare se la progettazione e la costruzione ne consentono l'installazione e la messa in servizio sicura.

- Il dossier tecnico non deve essere necessariamente costituito da un solo documento, ma deve essere comunque possibile ricostruirlo e renderlo disponibile in tempi ragionevoli. Deve essere disponibile per dieci anni dopo la produzione dell'ultima unità. L'impossibilità di renderlo disponibile in seguito a una richiesta giustificata da parte di un'autorità può costituire motivo di dubbio della conformità.

Il dossier tecnico non deve necessariamente comprendere piani dettagliati o altre informazioni specifiche sui sottogruppi usati per la produzione della macchina, a meno che non siano essenziali per verificare la conformità con i requisiti essenziali di sicurezza e salute.

Valutazione di conformità per le macchine dell'Allegato IV

Valutazioni di conformità

Alcuni tipi di attrezzature sono soggette a misure speciali. Queste attrezzature sono elencate nell'Allegato IV della direttiva e comprendono le macchine pericolose quali alcuni macchinari per la lavorazione del legno, presse, stampi, macchine per lavori sotterranei, ponti elevatori di veicoli, ecc.

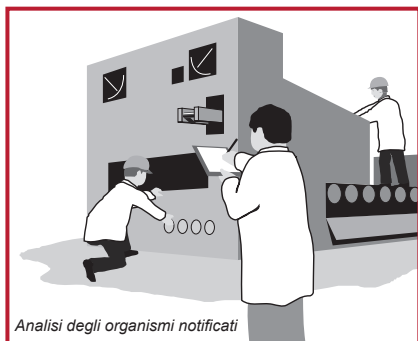
L'Allegato IV comprende inoltre alcuni componenti di sicurezza quali le barriere fotoelettriche e le unità di controllo a due mani.

Per le macchine di cui all'Allegato IV conformi agli standard armonizzati europei esistono tre procedure tra cui scegliere:

1. Inviare il dossier tecnico a un organismo notificato che confermerà la ricezione del dossier e lo conserverà. *Nota: con questa opzione, non è prevista alcuna valutazione del dossier. Il dossier può essere usato successivamente come riferimento in caso di problemi o di reclamo di non conformità.*

2. Inviare il dossier tecnico a un organismo notificato che verificherà la corretta applicazione degli standard armonizzati e fornirà un certificato di adeguatezza per il dossier.

3. Fornire un esempio della macchina a un organismo notificato (laboratorio di prova) per l'esame CE. Se l'esame viene superato, alla macchina sarà fornito il certificato di esame di tipo CE.

Analisi degli organismi notificati

Per le macchine dell'Allegato IV non conformi a uno standard o nel caso in cui non esista una norma armonizzata europea pertinente, occorre sottoporre un esempio della macchina a un organismo notificato (laboratorio di prova) che ne esegua l'esame CE.

Organismi notificati

Nell'ambito dello SEE e in alcuni altri paesi, esiste una rete di organismi notificati che comunicano tra di loro e lavorano con criteri comuni. Gli organismi notificati sono nominati dai governi (non dall'industria) e tutte le informazioni relative a queste organizzazioni sono rintracciabili su:

http://europa.eu.int/comm/enterprise/newapproach/legislation/nb/en 98-37-ec.pdf

Esame di tipo CE

Per eseguire un esame di tipo CE, l'organismo notificato necessita del dossier tecnico e deve avere accesso alla macchina da esaminare. Sarà verificato che la macchina è stata prodotta in conformità con il dossier tecnico e che soddisfa i criteri essenziali di sicurezza e salute pertinenti. Se l'esame viene superato, viene fornito un certificato di esame di tipo CE. Un ente che rifiuta di fornire un certificato deve informare gli altri organismi notificati.

Procedura per la dichiarazione di conformità CE

La persona responsabile deve redigere una Dichiarazione di Conformità CE e apporre il marchio CE a tutte le macchine fornite. Inoltre, le macchine devono essere fornite insieme alla Dichiarazione di Conformità CE.

Nota: i componenti di sicurezza devono avere una Dichiarazione di Conformità CE ma non è necessario il marchio CE, in base alla Direttiva Macchine (sebbene il marchio CE sia previsto dalle direttive EMC o Bassa Tensione).

Il marchio CE attesta che la macchina è conforme a tutte le Direttive Europee applicabili e che è stata sottoposta a tutte le corrispondenti procedure di valutazione della conformità. Apporre il marchio CE è un reato se la macchina non soddisfa i requisiti essenziali di sicurezza e salute ed è effettivamente sicura. Inoltre, è reato apporre un marchio che può essere confuso con il marchio CE.

Dichiarazione CE di incorporazione

Nei casi in cui le attrezzature sono fornite per essere assemblate con altri elementi al fine di costituire una macchina completa successivamente, la persona responsabile può fornire una DICHIARAZIONE DI INCORPORAZIONE (invece di una dichiarazione di conformità). Il marchio CE NON deve essere apposto. La dichiarazione dovrebbe affermare che l'attrezzatura non deve essere messa in servizio finché la macchina in cui sarà incorporata non sarà stata dichiarata conforme.

Questa opzione non è disponibile per le attrezzature che funzionano indipendentemente o che modificano la funzione della macchina.

Maykit Wright Ltd.
Dichiarazione di conformità

Nel rispetto delle seguenti Direttive:

Direttiva Macchine Europea 98/37/EC. (Qualunque altra direttiva pertinente alla macchina, ad esempio quella sulla compatibilità elettromagnetica EMC, dovrebbe essere inclusa.)

Società:

Maykit Wright Ltd.
Main Street
Anytown Industrial Estate
Anytown, England AB1 2DC
Tel: 00034 000890.
Fax: 00034

Macchina: Confezionatrice per carni.
Tipo: Vacustarwrap 7D
Numero di serie: 00516

Conforme alle norme: *(Tutte le pertinenti Norme Europee Armonizzate utilizzate e, dove applicabile, eventuali specifiche e norme nazionali.)*

Se la macchina è contemplata dall'Allegato IV, è necessario includere quanto segue:

– Il nome e l'indirizzo dell'Organismo notificato e il numero del Certificato di Esame di Tipo, oppure

– Il nome e l'indirizzo dell'Organismo notificato che ha rilasciato un Certificato di Adeguatezza per il dossier tecnico, oppure

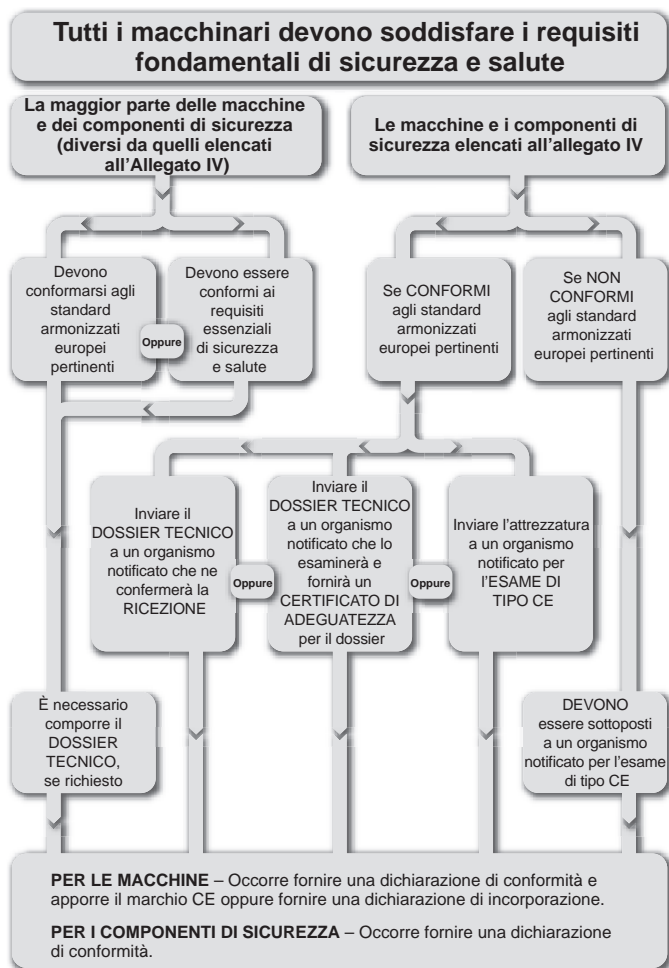
– Il nome e l'indirizzo dell'Organismo notificato a cui è stato inoltrato il dossier tecnico.

Questo per dichiarare che la macchina in oggetto è conforme ai pertinenti Requisiti Fondamentali di Salute e Sicurezza della Direttiva Macchine Europea 98/37/EC.

G. V. Wright

G.V. Wright, Amministratore Delegato
17 Gennaio 2003

Dichiarazione di Conformità di una macchina autocertificata

DIRETTIVA SULL'USO DELLE ATTREZZATURE DI LAVORO

Procedura schematica per la Direttiva Macchine

Mentre la Direttiva Macchine è indirizzata ai fornitori, questa Direttiva (89/655/EEC modificata 95/63/EC e 2001/45/EC) è rivolta agli utilizzatori delle macchine. Riguarda tutti i settori industriali e prevede sia obblighi generali per i datori di lavoro che requisiti minimi di sicurezza delle attrezzature di lavoro. Tutti i paesi SEE hanno recepito tale direttiva nelle proprie leggi nazionali per poterla applicare.

Per comprendere meglio il significato dei requisiti della Direttiva sull'Uso delle Attrezzature di Lavoro, è opportuno considerarne l'implementazione nelle legislazioni nazionali. Ci occuperemo della sua implementazione nel Regno Unito, con il nome di "The Provision and Use of Work Equipment Regulations" (P.U.W.E.R.). Il tipo di implementazione può variare tra i diversi paesi, ma l'effetto della direttiva rimane invariato.

Regolamenti da 1 a 10

Questi regolamenti forniscono i dettagli sui tipi di attrezzature e luoghi di lavoro coperti dalla direttiva.

Inoltre, prevedono doveri generali per i datori di lavoro, quali l'istituzione di sistemi sicuri di lavoro e la fornitura di attrezzature adeguate e sicure sottoposte a una corretta manutenzione. Gli operatori delle macchine devono ricevere informazioni e addestramento adeguati per un uso sicuro della macchina.

Le macchine nuove (e le macchine di seconda mano provenienti da paesi esterni allo SSE) fornite dopo il 1° gennaio 1993 devono soddisfare le direttive relative al prodotto pertinenti, ad esempio la Direttiva Macchine (questo è soggetto ad accordi transitori). Le attrezzature di seconda mano provenienti da paesi SEE fornite per la prima volta presso un dato posto di lavoro devono soddisfare immediatamente i regolamenti da 11 a 24.

Nota: le macchine esistenti o di seconda mano revisionate o modificate in modo significativo saranno classificate quali attrezzature nuove e gli interventi apportati devono garantire la conformità con la Direttiva Macchine (anche se si tratta di macchine per uso proprio della società).

Il Regolamento 5 "Adeguatezza delle attrezzature di lavoro" è il cuore della direttiva e sottolinea la responsabilità del datore di lavoro nella realizzazione di una corretta procedura di valutazione dei rischi.

Il Regolamento 6 "Manutenzione" prevede che la macchina sia sottoposta a manutenzione corretta. Normalmente, questo significa che deve esistere un piano di manutenzione ordinaria e preventiva pianificato. Si consiglia di compilare un registro e tenerlo aggiornato. Ciò è particolarmente importante quando la manutenzione e l'ispezione delle attrezzature contribuiscono alla costante integrità della sicurezza di un dispositivo o di un sistema di protezione.

Regolamenti da 11 a 24

Questi regolamenti riguardano rischi e misure di protezione specifiche delle macchine.

Per le macchine non modificate esistenti e in uso prima del 1° gennaio 1993, non sono stati completamente implementati fino al 1° gennaio 1997. Sono stati applicati con effetto immediato alle altre apparecchiature. Tuttavia, se le attrezzature sono conformi alle direttive relative al prodotto pertinenti, ad esempio la Direttiva Macchine, saranno automaticamente conformi ai regolamenti da 11 a 24, poiché la natura del loro contenuto è simile a quanto previsto dai requisiti essenziali di sicurezza e salute di tale direttiva.

Il regolamento 11, che prevede una gerarchia delle misure di protezione, è di particolare interesse. Le misure sono:

1. protezioni con recinzione fisse
2. altre protezioni o dispositivi di protezione
3. apparecchiature di protezione (dime, supporti, spingipezzo, ecc.)
4. la fornitura di informazioni, istruzioni, supervisione e formazione.

Queste misure devono essere applicate in sequenza, a partire dalla prima, per quanto possibile; in genere è richiesta una combinazione di almeno due punti.

Regolamenti USA

Questa sezione presenta alcuni dei regolamenti di sicurezza relativi alla protezione delle macchine industriali negli Stati Uniti. Si tratta solo di un punto di partenza; gli interessati dovranno approfondire ulteriormente i requisiti relativi alle proprie applicazioni e adottare le misure necessarie a garantire che progetti, procedure e metodi di uso e manutenzione rispondano alle proprie esigenze così come ai regolamenti e ai codici nazionali e locali.

Esistono numerose organizzazioni che promuovono la sicurezza industriale negli Stati Uniti. Queste includono:

1. società, che usano i requisiti stabiliti oltre a stabilire i propri requisiti interni;
2. la Occupational Safety and Health Administration (OSHA – Amministrazione per la salute a la sicurezza sul lavoro);
3. organizzazioni industriali quali la National Fire Protection Association (NFPA), la Robotics Industries Association (RIA) e la Association of Manufacturing Technology (AMT), oltre ai fornitori di soluzioni e prodotti di sicurezza quali Rockwell Automation.

OSHA (Occupational Safety and Health Administration)

Negli Stati Uniti, uno dei promotori principali della sicurezza industriale è la Occupational Safety and Health Administration (OSHA). L'OSHA è stata fondata nel 1970 da una legge del Congresso degli USA. Lo scopo di tale legge è garantire condizioni di lavoro sicure e igieniche e preservare le risorse umane. La legge autorizza il Secretary of Labor a definire standard obbligatori, relativi a sicurezza e salute sul lavoro, applicabili alle aziende che commerciano all'interno degli Stati Uniti. Questa legge si applica a tutti i posti di lavoro in uno Stato, nel Distretto di Columbia, nel Commonwealth di Porto Rico, nelle Isole Vergini, nelle Samoa Americane, a Guam, nel Territorio fiduciario delle Isole del Pacifico, nell'Isola di Wake, nelle Outer Continental Shelf Lands definite nell'Outer Continental Shelf Lands Act, nell'Isola Johnston e nella Zona del Canale di Panama.

L'articolo 5 della legge stabilisce i requisiti di base. Ogni datore di lavoro deve fornire, a ognuno dei suoi dipendenti, un lavoro e un posto di lavoro non soggetti a rischi conosciuti che provochino o possano provocare morte o gravi lesioni fisiche. Deve inoltre conformarsi agli standard relativi a salute e sicurezza sul lavoro promulgati da questa legge.

L'articolo 5, inoltre, stabilisce che ogni dipendente deve conformarsi agli standard relativi a salute e sicurezza sul lavoro e a tutte le regole, i regolamenti e gli ordini emessi in base a questa legge e applicabili alle proprie azioni e alla propria condotta.

La legge OSHA prevede responsabilità sia per il datore di lavoro sia per il dipendente. Decisamente diversa la Direttiva Macchine, che impone ai fornitori di immettere sul mercato macchine che non presentino pericoli. Negli Stati Uniti, un fornitore può vendere una macchina senza alcuna protezione. Spetta all'utente il compito di dotare la macchina delle protezioni necessarie a renderla sicura. Sebbene questa fosse una pratica comune quando la legge è stata approvata, la tendenza attuale è quella di fornire macchine dotate di protezioni, poiché concepire una macchina completa di tutti i dispositivi di sicurezza necessari è molto più economico che aggiungere le protezioni dopo la progettazione e la costruzione. Al fine di conformarsi agli standard, fornitori e utilizzatori dovranno comunicare in modo efficace in relazione ai requisiti di protezione, in modo da consentire la costruzione di macchine non solo sicure ma anche più produttive.

Il Secretary of Labor ha l'autorità di promulgare, come standard di salute e sicurezza sul lavoro, qualunque standard che goda di consenso nazionale e qualunque standard federale stabilito, a meno che la promulgazione di tale standard non risulti in un miglioramento delle condizioni di sicurezza e salute solo di certe categorie.

L'OSHA svolge questo ruolo pubblicando regolamenti al Titolo 29 del Code of Federal Regulation (29 CFR). Gli standard che riguardano le macchine industriali sono pubblicati dall'OSHA nella Parte 1910 del 29 CFR. Questi standard sono disponibili sul sito web OSHA – www.osha.gov. Diversamente da molti standard, la cui applicazione è volontaria, gli standard OSHA sono obbligatori di legge.

Alcune delle parti più importanti relative alla sicurezza delle macchine sono le seguenti:

A – Dati generali
B – Adozione ed estensione degli Established Federal Standards
C – Disposizioni generali su salute e sicurezza
H – Materiali pericolosi
I – Dispositivi di protezione personale
J – Controlli ambientali generali – tra cui Lockout/Tagout
O – Protezione delle macchine e dei macchinari
R – Settori speciali
S – Impianti elettrici

Alcuni standard OSHA incorporano, per riferimento, una serie di standard volontari. L'effetto legale dell'incorporazione per riferimento è che il materiale viene trattato come se fosse stato pubblicato per intero nel Federal Register. Quando uno standard che gode di consenso nazionale viene incorporato per riferimento in una delle sottoparti, è considerato obbligatorio. Ad esempio, l'NFPA 70, uno standard volontario conosciuto come US National Electric Code, è riportato nella Sottoparte S. Ciò rende obbligatori i requisiti contenuti nello standard NFPA70.

Il 29 CFR 1910.147, nella Sottoparte J, si occupa del controllo delle fonti di energia pericolosa. Si tratta di ciò che è più generalmente conosciuto come lo standard "Lockout/Tagout". Lo standard volontario corrispondente è ANSI Z244.1. Fondamentalmente, questo standard richiede che, prima degli interventi di assistenza e manutenzione, l'alimentazione della macchina venga scollegata e bloccata. Lo scopo è prevenire la messa in tensione o l'avviamento non previsti della macchina e i conseguenti infortuni ai danni dei lavoratori.

I datori di lavoro devono stabilire un programma e utilizzare precise procedure per la sistemazione di adeguati dispositivi di lockout o tagout sui dispositivi di isolamento dell'alimentazione e per disabilitare altrimenti le macchine o le apparecchiature in modo da impedirne la messa in tensione, l'avviamento o il rilascio di energia accumulata, involontari o imprevisti, ed evitare infortuni ai danni dei lavoratori.

Questo standard non copre modifiche e regolazioni di minore importanza e altre operazioni ordinarie che devono avvenire durante il normale funzionamento delle macchine se si tratta di interventi ripetitivi e sostanziali nell'utilizzo delle apparecchiature di produzione, ammesso che il lavoro sia svolto usando misure alternative che forniscano un'adeguata protezione. Come misure alternative si intendono dispositivi di protezione quali barriere fotoelettriche, pedane di sicurezza, interblocchi porte e altri simili dispositivi collegati a un sistema di sicurezza.

L'obiettivo, per il progettista di macchine e per l'utilizzatore, è determinare gli aspetti di "minore importanza" e quelli di "routine, ripetitivi e integranti nell'utilizzo".

La Sottoparte O è relativa alla protezione di macchine e macchinari ("Machinery and Machine Guarding"). Questa sottoparte elenca i requisiti generali per tutte le macchine e quelli di alcune particolari macchine. Dal 1970, anno in cui è stato costituito, l'OSHA ha adottato molti standard ANSI esistenti. Ad esempio B11.1 per le presse meccaniche è stato adottato come 1910.217.

1910.212 è lo standard generale OSHA per le macchine. Stabilisce che, per proteggere l'operatore e il personale vicino alla macchina da pericoli come quelli creati dal punto di lavoro, punti di intrappolamento, parti rotanti, schegge e scintille, occorre prevedere uno o più metodi di protezione. Le protezioni devono essere, quando possibile, installate sulla macchina o fissate in qualunque altro posto se, per qualche ragione, fosse impossibile farlo sulla macchina. La protezione deve essere tale da non costituire essa stessa un pericolo.

Il "punto di lavoro" è la zona della macchina in cui viene effettivamente lavorato il materiale. Il punto di lavoro di una macchina, il cui funzionamento espone il personale a rischio di lesioni, deve essere protetto. Il dispositivo di protezione deve essere conforme ai corrispondenti standard o, in assenza di specifici standard applicabili, deve essere concepito e costruito in modo tale da impedire che l'operatore introduca una qualunque parte del suo corpo nella zona di pericolo durante il ciclo operativo.

La Sottoparte S (1910.399) stabilisce i requisiti elettrici OSHA. Un'installazione o un'apparecchiatura è accettabile per l'Assistant Secretary of Labor e approvata, secondo i criteri di questa Sottoparte S, se è accettata, certificata, omologata, etichettata o altrimenti dichiarata sicura da un laboratorio di prova riconosciuto a livello nazionale (NRTL).

Che cos'è un'apparecchiatura? Un termine generale che include materiali, accessori, dispositivi, apparecchi, attrezzi di fissaggio, apparati e altri componenti simili usati come parte integrante di un'installazione elettrica o in collegamento ad essa.

Che cosa significa "omologata"? L'apparecchiatura è "omologata" se corrisponde al tipo menzionato in una lista che, (a) sia pubblicata da un laboratorio riconosciuto a livello nazionale che effettua periodiche ispezioni della produzione di tale apparecchiatura, e (b) attesti che tale apparecchiatura risponde agli standard riconosciuti a livello nazionale o è stata testata e riconosciuta sicura per l'uso designato.

A partire da Luglio 2006, le seguenti società sono laboratori di prova riconosciuti a livello nazionale:

- Applied Research Laboratories, Inc. (ARL)
- Canadian Standards Association (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- Electrical Reliability Services, Inc. (ERS)
- Entela, Inc. (ENT)
- FM Global Technologies LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TUV America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TUV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

Alcuni stati hanno adottato i propri OSHA locali. Ventiquattro stati, Porto Rico e le Isole Vergini hanno piani statali approvati dall'OSHA e hanno adottato propri standard e proprie politiche di implementazione. Nella maggior parte dei casi, questi stati adottano standard identici agli OSHA federali. Tuttavia, alcuni stati hanno adottato standard differenti o diverse politiche di implementazione.

I datori di lavoro devono riferire all'OSHA la storia degli incidenti. L'OSHA compila i tassi di incidenti, trasmette le informazioni agli uffici locali e utilizza queste informazioni per pianificare le ispezioni. I principali criteri di controllo sono:

- pericolo imminente
- catastrofi e fatalità
- reclami dei dipendenti
- industrie ad alto rischio
- ispezioni locali pianificate
- ispezioni di monitoraggio
- programmi a livello nazionale e locale

La violazione degli standard OSHA può comportare delle sanzioni. Violazioni e sanzioni sono classificate come segue:

- Grave: fino a 7.000 USD per violazione
- Non grave: a discrezione ma non oltre 7.000 USD
- Ripetuta: fino a 70.000 USD per violazione
- Intenzionale: fino a 70.000 USD per violazione
- Violazioni causa di decessi: ulteriori penali
- Mancato intervento: 7.000 USD/giorno

La tabella che segue mostra le prime 14 citazioni OSHA, da Ottobre 2004 a Settembre 2005.

Standard	**Descrizione**
1910.147	Il controllo delle fonti di energia pericolose (Lockout/Tagout)
1910.1200	Comunicazione dei pericoli
1910.212	Requisiti generali per tutte le macchine
1910.134	Protezione respiratoria
1910.305	Metodi di cablaggio, componenti e apparecchiature di uso generale
1910.178	Veicoli industriali a motore
1910.219	Trasmissione meccanica
1910.303	Requisiti generali
1910.213	Macchinari di lavorazione del legno
19102.215	Mole abrasive
19102.132	Requisiti generali
1910.217	Presse meccaniche
1910.095	Esposizione al rumore sul luogo di lavoro
1910.023	Protezione di fori e aperture a muro e a pavimento

Regolamenti canadesi

In Canada, la sicurezza industriale è governata a livello provinciale. Ogni provincia mantiene e applica i propri regolamenti. L'Ontario, ad esempio, ha promulgato l'Occupational Health and Safety Act che stabilisce i diritti e i doveri di tutti i soggetti sul luogo di lavoro. Il suo scopo principale è quello di proteggere i lavoratori contro i pericoli per la salute e la sicurezza sul lavoro. La legge definisce una serie di procedure atte a gestire i rischi sul posto di lavoro e ne impone l'implementazione per legge nei casi in cui ciò non avvenga volontariamente.

La legge include il regolamento 851, sezione 7, che definisce l'analisi delle condizioni di preavviamento relative a salute e sicurezza. Questa analisi è un requisito dell'Ontario per qualunque componente di macchinari nuovo, ricostruito o modificato, per cui un tecnico professionista deve redigere un rapporto.

Standard

Questa sezione fornisce una lista di alcuni tipici standard, internazionali e nazionali, relativi alla sicurezza delle macchine. Non vuole essere un elenco esaustivo ma dare piuttosto una visione d'insieme sulle problematiche di sicurezza delle macchine che sono oggetto di standardizzazione.

Questo capitolo dovrebbe essere letto insieme al Capitolo 1.

Tutti i paesi stanno lavorando per l'armonizzazione globale degli standard. Ciò è particolarmente evidente nel campo della sicurezza delle macchine. Gli standard di sicurezza globali per le macchine sono governati da due organizzazioni: ISO e IEC. Le norme regionali e nazionali sono ancora in vigore e continuano a supportare i requisiti locali ma, in molti paesi, si è affermata una tendenza all'uso di standard internazionali redatti da ISO e IEC.

Le norme EN (European Norm), ad esempio, vengono utilizzate in tutti i paesi EEA. Tutte le nuove norme EN sono allineate con le norme ISO e IEC e, in molti casi, presentano un testo identico.

L'IEC tratta le problematiche elettrotecniche e l'ISO si occupa di tutte le altre questioni. Molti paesi industrializzati sono membri di IEC e ISO. Gli standard di sicurezza per le macchine sono redatti da gruppi di lavoro costituiti da esperti dei vari paesi industrializzati del mondo.

In molti paesi, gli standard possono essere considerati volontari mentre i regolamenti sono legalmente obbligatori. Tuttavia, gli standard vengono solitamente utilizzati come interpretazione pratica dei regolamenti. Quindi, l'ambito degli standard e quello dei regolamenti sono strettamente interrelati.

Consultare il catalogo sulla sicurezza disponibile su: www.ab.com/safety per una lista completa degli standard.

ISO (International Organization for Standardization)

L'ISO è una organizzazione non governativa costituita da organismi di normazione nazionali di molti paesi (157 attualmente). Una Segreteria Centrale situata a Ginevra, in Svizzera, coordina il sistema. L'ISO elabora standard atti a progettare, costruire e utilizzare le macchine in modo più efficiente, più sicuro e più pulito. Gli standard, inoltre, facilitano e rendono più trasparente il commercio tra i diversi paesi.

Gli standard ISO possono essere identificati dalle tre lettere ISO

Gli standard ISO per le macchine sono organizzati come gli standard EN, in tre livelli: Tipo A, B e C (v. l'ultima sezione sulle Norme Armonizzate Europee EN).

Per ulteriori informazioni, visitare il sito web ISO: www.iso.org.

IEC (International Electrotechnical Commission)

L'IEC redige e pubblica standard internazionali per impianti elettrici, elettronici e relative tecnologie. Attraverso i suoi membri, l'IEC promuove la collaborazione internazionale su tutte le questioni di standardizzazione elettrotecnica e temi collegati, come la valutazione della conformità agli standard elettrotecnici.

Per ulteriori informazioni, visitare il sito web IEC: www.iec/ch

Norme europee armonizzate EN

Questi standard sono condivisi da tutti i paesi SEE e sono redatti dagli enti di normazione europei CEN e CENELEC. Il loro uso è volontario ma progettare e produrre le apparecchiature in base a questi standard è il modo più semplice e diretto per dimostrare la conformità ai requisiti fondamentali di sicurezza e salute.

Sono suddivisi in 3 tipi: standard A, B e C.

STANDARD di Tipo A: trattano aspetti relativi a tutti i tipi di macchina.

STANDARD di Tipo B: sono suddivisi in 2 gruppi.
STANDARD di Tipo B1: trattano aspetti di sicurezza ed ergonomicità specifici dei macchinari.
STANDARD di Tipo B2: riguardano i componenti di sicurezza e i dispositivi di protezione.

STANDARD di Tipo C: riguardano tipi o gruppi specifici di macchine.

È importante notare che la conformità con uno standard C implica automaticamente la presunzione di conformità con i requisiti essenziali di sicurezza e salute. In assenza di uno standard C pertinente, è possibile usare gli standard A e B come prova totale o parziale della conformità ai requisiti essenziali evidenziando il rispetto delle sezioni pertinenti.

Il sistema solare può essere usato come modello per illustrare le relazioni tra la Direttiva Macchine e gli standard europei. I pianeti rappresentano gli standard, che ruotano intorno al sole, che rappresenta la Direttiva Macchine. Le orbite interne sono gli standard A e B, mentre quelle esterne sono gli standard C.

Per la collaborazione tra CEN/CENELEC e organismi come ISO e IEC, è stata stipulata una serie di accordi miranti alla definizione di standard comuni a livello mondiale. In molti casi, uno standard EN ha uno standard analogo in IEC o ISO. In generale, i due testi sono uguali ed eventuali differenze locali vengono presentate nella premessa dello standard.

Il capitolo 2 elenca alcuni standard EN/ISO/IEC e altri standard nazionali e regionali relativi alla sicurezza delle macchine. Quando uno standard EN è riportato tra parentesi, significa che è identico o molto simile allo standard ISO o IEC. Per una lista completa degli standard EN sulla sicurezza delle macchine, accedere a:
http://europa.eu.int/comm/enterprise/mechan_equipment/machinery/index.htm.

Standard USA

Standard OSHA

Quando possibile, l'OSHA promulga standard a consenso nazionale o standard federali stabiliti come standard di sicurezza. Le disposizioni obbligatorie (ad es. la parola "deve" implica il carattere obbligatorio) degli standard incorporati per riferimento hanno la stessa forza e lo stesso effetto degli standard elencati nella Parte 1910. Ad esempio, lo standard a consenso nazionale NFPA 70 è riportato come documento di riferimento nell'Appendice A della Sottoparte S-Impianti elettrici della Parte 1910 del 29 CFR. NFPA 70 è uno standard volontario sviluppato dalla National Fire Protection Association (NFPA). La NFPA 70 è conosciuta anche come National Electric Code (NEC). Per incorporazione, tutti i requisiti obbligatori del NEC sono obbligatori anche per l'OSHA.

Standard ANSI

L'American National Standards Institute (ANSI) funge da amministratore e coordinatore del sistema di standardizzazione volontario del settore privato degli Stati Uniti. Si tratta di un'organizzazione di membri privata e senza scopo di lucro sostenuta da numerose organizzazioni del settore pubblico e privato.

ANSI non si occupa propriamente della creazione degli standard ma ne facilita lo sviluppo promuovendone il consenso tra gruppi qualificati. ANSI, inoltre, garantisce che tutti i gruppi qualificati rispettino i principi di consenso, correttezza dei processi e trasparenza. Di seguito è riportato un elenco parziale degli standard di sicurezza industriale che si possono ricevere contattando l'ANSI.

Questi standard si distinguono tra standard applicativi e standard costruttivi. Gli standard applicativi determinano il modo in cui applicare una protezione di sicurezza alla macchina. Alcuni esempi sono l'ANSI B11.1, che fornisce informazioni su come usare le protezioni sulle presse e l'ANSI/RIA R15.06, che descrive l'uso dei dispositivi di sicurezza per la protezione dei robot.

NFPA (National Fire Protection Association)

La National Fire Protection Association (NFPA) è stata costituita nel 1896. La sua missione è ridurre i danni causati dagli incendi migliorando la qualità della vita tramite l'uso di codici consensuali e standard basati su dati scientifici, la ricerca e l'addestramento in merito alle problematiche riguardati il fuoco e la sicurezza. La NFPA promuove l'uso di numerosi standard che aiutino a realizzare tale missione. Due standard molto importanti correlati alla sicurezza industriale e alla salvaguardia sono il National Electric Code (NEC) e l'Electrical Standard for Industrial Machinery.

L'NFPA agisce in qualità di sostenitore del NEC fin dal 1911. Il documento del codice originale è stato sviluppato nel 1897 in seguito allo sforzo congiunto di vari interessi legati a diversi settori, tra cui quello elettrico, edilizio e delle assicurazioni. Da allora, il NEC è stato aggiornato diverse volte e viene revisionato ogni tre anni circa. L'articolo 670 del NEC contiene alcuni dettagli relativi ai macchinari industriali e fa riferimento all'Electrical Standard for Industrial Machinery, NFPA 79.

NFPA 79 si applica ad attrezzature, apparati o sistemi di macchine industriali elettrici/elettronici che operano a una tensione pari a un massimo di 600 Volt. Lo scopo del NFPA 79 è fornire informazioni dettagliate per l'applicazione di attrezzature, apparati o sistemi elettrici/elettronici che fanno parte di macchinari industriali in modo tale da promuovere la sicurezza di beni e persone. L'NFPA 79, adottato ufficialmente da ANSI nel 1962, è molto simile nel contenuto allo standard IEC 60204-1.

Le macchine che non sono coperte da standard specifici OSHA devono essere prive dei rischi riconosciuti e che possono provocare il decesso o danni personali gravi. Tali macchine devono essere progettate e sottoposte a manutenzione almeno conformemente agli standard industriali applicabili. NFPA 79 è uno standard che si applica alle macchine non specificamente coperte dagli standard OSHA.

Standard canadesi

Gli standard CSA riflettono il consenso nazionale di produttori e utilizzatori – tra cui costruttori, consumatori, rivenditori, sindacati, organizzazioni professionali e agenzie governative. Gli standard sono ampiamente usati dall'industria e dal commercio e, spesso, adottati nei regolamenti di governi municipali, provinciali e federali, soprattutto nei campi della salute, della sicurezza, dell'edilizia e dell'ambiente.

Privati, società e associazioni di tutto il Canada sostengono attivamente lo sviluppo degli standard CSA, dedicando, in qualità di volontari, tempo e capacità al lavoro del Comitato CSA e supportando gli obiettivi dell'associazione attraverso la loro attiva partecipazione. Il CSA può contare, in totale, su più di 7000 volontari dei comitati e 2000 soci sostenitori.

Lo Standards Council of Canada è l'organo di coordinamento del sistema National Standards, una federazione di organizzazioni indipendenti e autonome che lavorano per l'ulteriore sviluppo e miglioramento della standardizzazione volontaria, nell'interesse nazionale.

Standard australiani

Molti di questi standard sono strettamente allineati con gli equivalenti standard ISO/IEC/EN

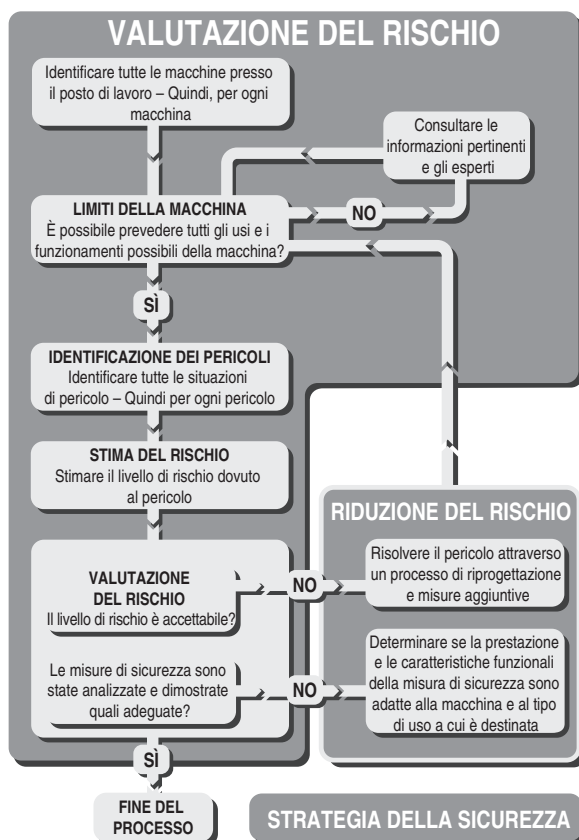
Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001
Telefono: +61 2 8206 6000
E-mail: mail@standards.org.au
Sito web: www.standards.org.au

Per acquistare copie degli standard:
SAI Global Limited
286 Sussex Street, Sydney, NSW 2001
Telefono: +61 2 8206 6000
Fax. +61 2 8206 6001
E-mail: mail@sai-global.com
Sito web: www.saiglobal.com/shop

Consultare il catalogo sulla sicurezza disponibile in: www.ab.com/safety per una lista completa degli standard.

Strategia della sicurezza

Da un punto di vista puramente funzionale, maggiore è l'efficienza di una macchina nello svolgere la propria attività di lavorazione dei materiali, migliore essa è. Tuttavia, affinché una macchina sia utilizzabile deve anche essere sicura. La sicurezza deve certamente essere considerata di primaria importanza.

Per individuare la corretta strategia di sicurezza, è necessaria l'interazione di due fasi chiave, come mostrato di seguito.

La **VALUTAZIONE DEI RISCHI**, basata su una chiara comprensione dei limiti e delle funzioni della macchina e delle attività che la macchina può dover svolgere durante la sua vita operativa.

La **RIDUZIONE DEI RISCHI** viene eseguita se necessario e le misure di sicurezza vengono selezionate in base alle informazioni ricavate dalla fase di valutazione del rischio.

Il modo in cui questo viene fatto rappresenta la base della STRATEGIA DELLA SICUREZZA per la macchina.

È necessario un elenco di controllo da seguire per garantire che tutti gli aspetti siano presi in considerazione e che il principio fondamentale non venga perso di vista nei dettagli. Innanzitutto l'intero processo dovrebbe essere documentato. Questo non solo assicura l'esecuzione di un lavoro più accurato, ma consente anche di rendere disponibili i risultati affinché siano controllati da terzi.

Questa sezione è rivolta sia ai costruttori sia agli utilizzatori di macchine. Il costruttore deve garantire che la macchina possa essere utilizzata in sicurezza. La valutazione dei rischi dovrebbe essere iniziata in fase di progettazione e dovrebbe considerare tutte le prevedibili attività che la macchina dovrà svolgere. Questo approccio basato sulle attività, nella fase preliminare di valutazione dei rischi, è molto importante. Ad esempio, può esserci l'esigenza di regolare le parti mobili della macchina. In fase progettuale, dovrebbe essere possibile prevedere misure che consentano di realizzare in sicurezza queste operazioni. Se ciò non avviene in una fase preliminare, può essere difficile o impossibile farlo in una fase successiva. Il risultato potrebbe essere che la regolazione delle parti mobili deve comunque essere realizzata ma in mancanza di sicurezza o in modo inefficiente (o entrambi). Una macchina per la quale siano stati considerati tutte le attività durante la valutazione dei rischi sarà più sicura ed efficiente.

L'utilizzatore (o il datore di lavoro) deve garantire che le macchine, nell'ambiente di lavoro, siano sicure. Anche se una macchina è stata dichiarata sicura dal costruttore, l'utilizzatore dovrebbe comunque procedere a una valutazione dei rischi per determinare se l'apparecchiatura è sicura nel proprio ambiente di installazione. Le macchine vengono spesso usate in circostanze che il costruttore non può prevedere. Ad esempio, una fresatrice usata in un laboratorio scolastico richiederà che vengano fatte ulteriori considerazioni rispetto al caso di una fresa usata in un'officina industriale.

Occorre inoltre ricordare che se una società utilizzatrice acquista due o più macchine indipendenti e le integra all'interno di un processo, diventa a sua volta produttrice della macchina combinata risultante.

Vediamo ora i passaggi principali verso la definizione di una adeguata strategia di sicurezza. Quanto segue può essere applicato alle installazioni già esistenti in fabbrica o a una macchina nuova singola.

Valutazione dei rischi

È errato considerarla come un onere. È invece una procedura utile che fornisce informazioni essenziali e consente all'utente o al progettista di prendere decisioni ragionate sui metodi per garantire la sicurezza.

Esistono vari standard che trattano questo argomento. ISO 14121: "Principi per la valutazione dei rischi" e ISO 12100: "Sicurezza delle macchine – Principi di base" contiene le istruzioni più utilizzate a livello globale.

Qualunque sia la tecnica usata per la valutazione dei rischi, un team interfunzionale di persone arriverà a un risultato più esaustivo ed equilibrato rispetto a un singolo.

La valutazione dei rischi è un processo iterativo che deve essere realizzato in diverse fasi del ciclo di vita della macchina. Le informazioni disponibili varieranno in base alla fase del ciclo di vita. Ad esempio, una valutazione dei rischi condotta da un costruttore potrà avvalersi di ogni dettaglio sui meccanismi della macchina e sui materiali di costruzione ma, probabilmente, potrà soltanto ipotizzare l'ambiente di lavoro finale della macchina. D'altra parte, una valutazione dei rischi effettuata dall'utilizzatore della macchina non entrerà nel merito di tutti i dettagli tecnici ma potrà considerare con precisione l'ambiente di lavoro della macchina. Idealmente, il risultato di una iterazione è l'input per l'iterazione successiva.

Determinazione dei limiti della macchina

Ciò comporta la raccolta e l'analisi di informazioni sui pezzi, sui meccanismi e sulle funzioni di una macchina. Inoltre, sarà necessario considerare tutti i tipi di interazione umana con la macchina e l'ambiente in cui questa opererà. L'obiettivo è una chiara comprensione della macchina e delle sue modalità d'uso.

Le macchine che vengono collegate, meccanicamente o mediante sistemi di controllo, dovrebbero essere considerate come un'unica macchina, a meno che non siano "separate a zone" da adeguate misure di protezione.

È importante tener conto di tutti i limiti e di tutte le fasi della vita di una macchina, compresa l'installazione, la messa in servizio, la manutenzione, la messa fuori servizio, l'uso corretto e il funzionamento, oltre alle conseguenze di malfunzionamenti e usi errati prevedibili.

Identificazione delle attività e dei pericoli

Tutti i pericoli inerenti alla macchina devono essere identificati ed elencati in base alla loro natura e posizione. I tipi di pericolo includono schiacciamento, taglio, intrappolamento, espulsione di pezzi, emissione di fumi, radiazioni, sostanze tossiche, calore, rumore ecc.

I risultati dell'analisi delle attività dovrebbero essere confrontati con quelli dell'identificazione dei pericoli. Ciò servirà a evidenziare l'eventuale compresenza di un pericolo e di una persona, ossia una situazione pericolosa. Tutte le situazioni pericolose dovrebbero essere riportate in un elenco. A seconda della natura della persona o dell'attività, è possibile che lo stesso pericolo possa produrre diversi tipi di situazioni pericolose. La presenza di un tecnico di manutenzione altamente esperto e qualificato, ad esempio, può avere implicazioni diverse rispetto alla presenza di un addetto alle pulizie senza esperienza, che non conosce la macchina. In queste situazioni, se ogni caso viene elencato e affrontato separatamente, è possibile giustificare misure di protezione diverse per il tecnico di manutenzione e l'addetto alle pulizie. Se i casi non vengono elencati e affrontati separatamente, bisognerebbe fare riferimento al caso di rischio più grave e, di conseguenza, tecnico di manutenzione e addetto alle pulizie sarebbero coperti dalla stessa misura di protezione.

A volte sarà necessario effettuare una valutazione generale dei rischi su macchine già esistenti, già dotate di misure di protezione (ad es. una macchina con parti mobili pericolose protette da una porta interbloccata). Le parti mobili sono un rischio potenziale che può diventare un pericolo effettivo in caso di rottura del sistema di interblocco. A meno che il sistema di interblocco non sia già stato convalidato (attraverso la valutazione dei rischi o una progettazione rispondente a determinati standard), la sua presenza non dovrebbe essere presa in considerazione.

Stima del rischio

Questo è uno degli aspetti più importanti della valutazione dei rischi. Ci sono molti modi di affrontare questo aspetto e, nelle pagine che seguono, se ne illustrano i principi di base.

Qualunque macchina che possa creare situazioni pericolose presenta un rischio di evento pericoloso (ad es. lesioni). Maggiore è il rischio, maggiore è l'importanza di un adeguato intervento. Per un determinato pericolo, il rischio potrebbe essere così ridotto da poter essere tollerato e accettato ma, per un altro pericolo, il rischio potrebbe essere così elevato da rendere indispensabile l'adozione di misure estreme di protezione. Quindi, per prendere una decisione sulla necessità e sul tipo di intervento, occorre essere in grado di quantificare il rischio.

Il rischio viene spesso inteso esclusivamente in termini di gravità delle lesioni in caso di incidente. SIA la gravità del danno potenziale SIA la probabilità che si verifichi devono essere prese in considerazione per stimare la gravità del rischio presente.

Il metodo proposto nelle pagine successive per la valutazione del rischio non è l'unico metodo possibile poiché circostanze diverse potrebbero richiedere approcci diversi. È PRESENTATO SOLO COME LINEA GUIDA GENERALE VOLTA A INCORAGGIARE L'USO DI UNA STRUTTURA METODICA E DOCUMENTATA.

Il sistema a punti utilizzato non è stato calibrato per particolari tipi di applicazione e quindi, in alcuni casi, può non essere adatto. È ora disponibile il Rapporto tecnico ISO TR 14121-2 "Risk assessment – Practical guidance and examples of methods" che fornisce le istruzioni pratiche più importanti.

Le seguenti informazioni servono a spiegare e a illustrare la sezione relativa alla stima dei rischi dell'attuale standard ISO 14121 "Principi per la valutazione dei rischi."

Vengono presi in considerazione i seguenti fattori:

- LA GRAVITÀ DELLE LESIONI POTENZIALI.
- LA PROBABILITÀ CHE SI VERIFICHINO.

La probabilità di occorrenza comprende due fattori:

- FREQUENZA DELL'ESPOSIZIONE.
- PROBABILITÀ DI LESIONI.

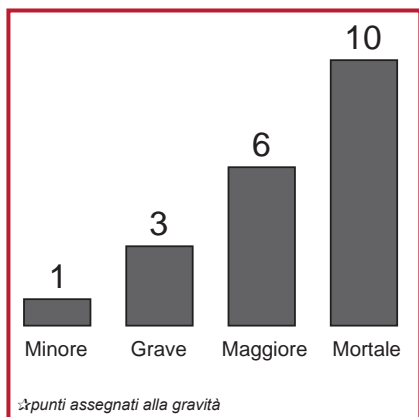
Assegneremo dei valori a ognuno di questi fattori analizzandoli separatamente.

Occorre sfruttare tutti i dati e le esperienze a disposizione. Poiché vengono considerate tutte le fasi di vita della macchina, per evitare troppa complessità, è necessario basare le decisioni sul caso più grave per ogni fattore.

È inoltre importante usare il buon senso. Le decisioni devono basarsi su azioni fattibili, realistiche e plausibili. Questo è il motivo per cui è utile l'approccio da parte di un team interfunzionale.

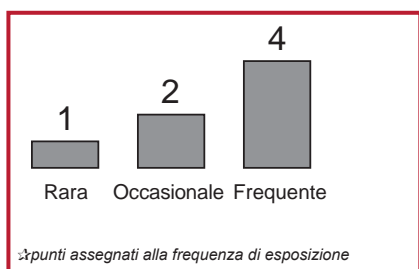
Ai fini di questo esercizio, non bisognerebbe considerare eventuali sistemi di protezione esistenti. Se la stima dei rischi rivela l'esigenza di un sistema di protezione, attraverso una serie di metodologie, è possibile determinarne le caratteristiche (v. più avanti in questo capitolo).

1. Gravità delle lesioni potenziali

In questo caso si presume che l'incidente o il danno si sia verificato, forse come conseguenza del pericolo. Lo studio accurato del pericolo rivelerà qual è il maggior danno possibile. Ricordare: in questo caso si presume che il danno sia inevitabile e ci si concentra solo sulla sua gravità. Occorre presumere che l'operatore sia esposto al movimento o al processo pericoloso. La gravità del danno deve essere valutata quale:

- FATALE: Morte
- IMPORTANTE: (generalmente irreversibile) disabilità permanente, perdita della vista, amputazione di arti, danni respiratori, ecc.
- GRAVE: (generalmente reversibile) perdita di conoscenza, ustioni, fratture, ecc.
- MINORE: ematomi, tagli, lievi abrasioni, ecc.

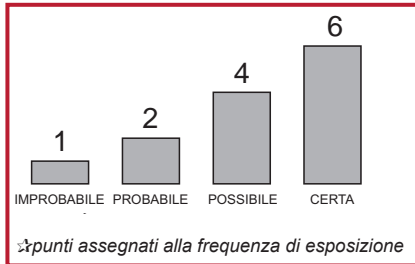
A ogni descrizione viene assegnato un valore, come illustrato.

2. Frequenza dell'esposizione

La frequenza di esposizione risponde alla domanda "Quanto spesso l'operatore o il tecnico di manutenzione è esposto al pericolo?". La frequenza di esposizione al pericolo può essere classificata come:

- FREQUENTE: più volte al giorno.
- OCCASIONALE: una volta al giorno.
- RARA: una volta a settimana o meno.

A ogni descrizione viene assegnato un valore, come illustrato.

3. Probabilità di lesioni

Occorre presumere che l'operatore sia esposto al movimento o al processo pericoloso. Se si considera il modo in cui l'operatore interagisce con la macchina e altri fattori (velocità di avviamento, ad esempio) è possibile classificare la probabilità di danno come:

- IMPROBABILE
- PROBABILE
- POSSIBILE
- CERTA

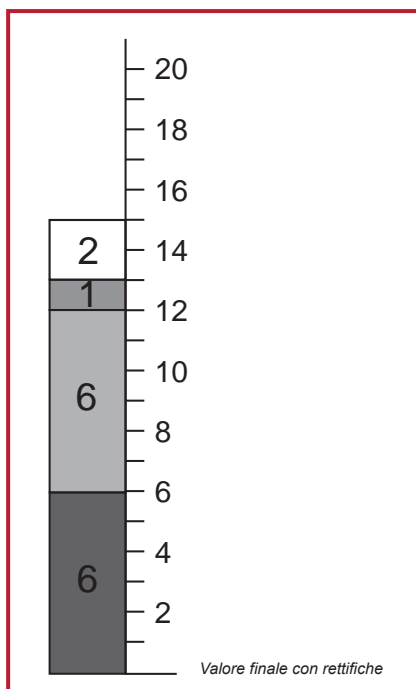
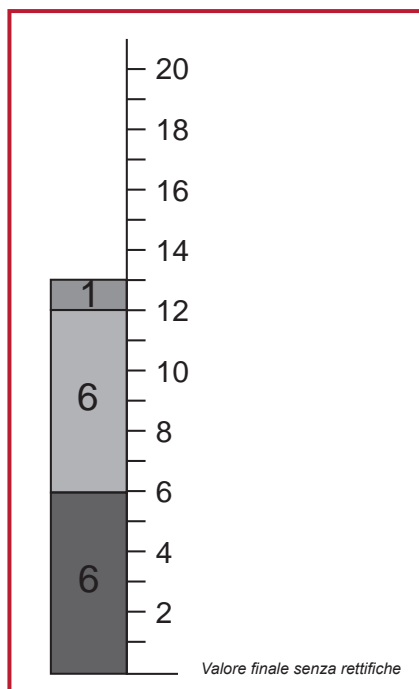
A ogni descrizione viene assegnato un valore, come illustrato.

A tutte le descrizioni viene assegnato un valore; tali valori sono quindi sommati per ottenere una stima iniziale. La somma dei tre componenti ammonta a un valore di 13. Ma dobbiamo considerare altri fattori. (Nota: questo non è necessariamente basato sulle illustrazioni precedenti).

Il prossimo passaggio prevede l'affinamento della stima iniziale prendendo in considerazione fattori aggiuntivi quali quelli illustrati nella seguente tabella. Spesso possono essere analizzati correttamente solo quando la macchina è installata nella sua postazione permanente.

Fattore tipico	**Azione proposta**
Più di una persona esposta al pericolo.	Moltiplicare il fattore di gravità per il numero di persone.
Periodo protratto nella zona pericolosa senza isolamento completo dell'alimentazione.	Se il tempo per ogni accesso è superiore a 15 minuti, aggiungere 1 punto al fattore di frequenza.
L'operatore non è esperto o addestrato.	Aggiungere 2 punti al totale.
Intervalli molto lunghi (ad esempio 1 anno) tra gli accessi. (Potrebbero verificarsi avarie progressive e non rilevate, soprattutto nei sistemi di monitoraggio).	Aggiungere i punti equivalenti al massimo fattore di frequenza.

Considerazioni aggiuntive per la stima dei rischi

I risultati di ogni fattore aggiuntivo devono essere sommati al totale precedente, come illustrato.

Riduzione dei rischi

Ora occorre prendere in considerazione ogni macchina e i rispettivi rischi e attuare le misure necessarie per risolverne tutti i rischi.

La tabella che segue è un esempio di una parte di un processo documentato per tenere conto di tutti gli aspetti legati alla sicurezza della macchina utilizzata. Serve da guida agli utilizzatori della macchina, ma anche i costruttori o i fornitori possono usare lo stesso principio per verificare che tutte le apparecchiature siano state convalidate. Inoltre, servirà da indice a rapporti più dettagliati sulla valutazione dei rischi.

Mostra che, nel caso in cui a una macchina sia stato apposto il marchio CE, il processo è più semplice poiché i rischi per la macchina sono già stati valutati dal produttore e tutte le misure necessarie sono già state attuate. Anche nel caso di attrezzature marchiate CE è possibile che siano presenti ulteriori rischi dovuti alla natura della sua applicazione o ai materiali lavorati non previsti dal produttore.

Società – MAYKIT WRIGHT LTD
Stabilimento – Tool room – East Factory.
Data – 8/29/95
Profilo operatore – esperto.

Descrizione apparecchiature e data	Conformità alle Direttive	Numero report di valutazione dei rischi	Storico incidenti	Note	Descrizione pericolo	Tipo di pericolo	Azione richiesta	Implementata e ispezionata – Riferimento
Tornio parallelo Bloggs. N. di serie. 8390726 Installato 1978	Nessuna richiesta	RA302	Nessuno	L'apparecchiatura elettrica è conforme a BS EN 60204 Pulsanti di emergenza montati (sostituiti 1989)	Rotazione mandrino con protezione aperta	Intrappolamento Taglio	Montaggio interruttore di interblocco di protezione	11/25/94 J Kershaw – Report n. 9567
					Fluido di taglio	Tossicità	Sostituire con tipo non tossico	11/30/94 J Kershaw – Report n. 9714
					Pulizia sfridi	Taglio	Fornire guanti	11/30/94 J Kershaw – Report n. 9715
Fresatrice a torretta Bloggs N. di serie 17304294 Fabbricata 1995 Installata Maggio 95	Dir. Macchine Dir. EMC	RA416	Nessuno		Movimento slitta (verso la parete)	Schiaccia-mento	Spostare la macchina per assicurare spazio sufficiente	4/13/95 J Kershaw – Report n. 10064

Gerarchia delle misure per la riduzione dei rischi

Esistono tre metodi di base, da considerare e usare nel seguente ordine:

1. eliminare o ridurre i rischi nella maggiore misura possibile (progettazione e costruzione di macchine intrinsecamente sicure)

2. installare i sistemi e le misure di protezione necessari (ad es. protezioni interbloccate, barriere fotoelettriche, ecc.) in relazione ai rischi che non possono essere eliminati in fase progettuale

3. informare gli utenti dei rischi residui dovuti a eventuali lacune delle misure protettive adottate, indicare l'addestramento necessario e specificare l'eventuale necessità di fornire al personale equipaggiamento protettivo aggiuntivo.

Ogni misura di questa gerarchia deve essere presa in considerazione partendo dall'inizio dell'elenco e usata laddove possibile. Questo approccio conduce, di solito, all'uso contemporaneo di più misure.

Progettazione a sicurezza intrinseca

Nella fase di progettazione della macchina, è possibile evitare molti dei possibili rischi semplicemente mediante l'attenta considerazione di fattori come i materiali, i requisiti di accesso, le superfici calde, i metodi di trasmissione, i punti di intrappolamento, i livelli di tensione, ecc.

Ad esempio, se non è necessario accedere a una zona pericolosa, la soluzione è proteggerla all'interno della macchina o con qualche tipo di protezione fissa.

Misure e sistemi di protezione

Se accedere alla zona pericolosa è necessario, la soluzione sarà un po' più complessa. Sarà necessario garantire che l'accesso sia possibile solo con la macchina in condizioni di sicurezza. Saranno necessarie misure protettive quali porte di protezione interbloccate e/o sistemi di sgancio. La scelta del dispositivo o sistema protettivo deve essere fortemente determinata dalle caratteristiche operative della macchina. Questo è estremamente importante, poiché un sistema che impedisce l'efficienza della macchina sarà soggetto a essere rimosso senza autorizzazione o ignorato.

In questo caso, la sicurezza della macchina dipende dalla corretta applicazione e dal funzionamento corretto del sistema protettivo anche in condizioni di guasto.

Adesso occorre esaminare il funzionamento corretto di tale sistema. Per ogni tipo di sistema esistono numerose tecnologie con diversi gradi di prestazione per il monitoraggio, il rilevamento e la prevenzione dei guasti.

In un mondo ideale tutti i sistemi protettivi sarebbero perfetti e non consentirebbero alcuna possibilità di guasto in condizioni pericolose. Nel mondo reale, tuttavia, siamo limitati dalla nostra conoscenza imperfetta e dai materiali adoperati. Un altro vincolo rilevante è il costo. In base a questi fattori, è chiaro che occorre utilizzare un certo senso delle proporzioni. Sarebbe ridicolo insistere che l'integrità di un sistema protettivo di una macchina che, nel peggiore dei casi, può provocare un ematoma, sia la stessa richiesta per un jumbo jet che vola a chilometri di distanza da terra. Le conseguenze di un eventuale guasto del sistema sono drasticamente diverse e dunque è necessario poter in qualche modo correlare la portata delle misure protettive al livello di rischio calcolato durante la fase di stima.

Qualunque sia il dispositivo protettivo prescelto, occorre ricordare che un "sistema di sicurezza" può comprendere numerosi elementi, tra cui il dispositivo di protezione, il cablaggio, un dispositivo di commutazione e a volte componenti del sistema di controllo operativo della macchina. Tutti questi elementi del sistema (comprese protezioni, montaggio, cablaggio, ecc.) devono presentare prestazioni e caratteristiche adatte alla propria progettazione e tecnologia. La versione pre-revisione dello standard ISO 13849-1 delinea varie categorie per i componenti di sicurezza dei sistemi di controllo e, nell'Allegato B, fornisce un grafico del rischio. Si tratta di un approccio molto semplicistico ma che può fornire una guida utile per determinare alcuni dei requisiti di un sistema di protezione.

Le versioni revisionate di ISO 13849-1 e IEC 62061 forniscono entrambe utili metodi e consigli su come definire un sistema di controllo legato alla sicurezza, ossia un sistema che costituisce una misura di protezione o svolge una funzione di sicurezza.

EN ISO 13849-1:2008, nell'Allegato A, fornisce un grafico migliore del rischio.

IEC 62061, nell'Allegato A, propone il metodo di seguito illustrato.

Valutazione del rischio e misure di sicurezza

Documento N.:
Parte di:

Prodotto: __________
Rilasciato da: __________
Data: __________

Area nera = Misure di sicurezza richieste
Area grigia = Misure di sicurezza raccomandate

☐ Valutazione preliminare del ri
☐ Valutazione intermedia del ri
☐ Valutazione di verifica del ris

Conseguenze	Severità Se	Classe Cl 3 – 4	5 – 7	8 – 10	11 – 13	14 – 15	Frequenza e durata, Fr		Probabilità evento di pericolo, Pr		Schiva
Morte, perdita di un occhio o di un braccio	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	< = 1 ora	5	Comune	5	
Permanente, perdita delle dita	3		OM	SIL 1	SIL 2	SIL 3	> 1 h – < = g.	5	Probabile	4	
Reversibile, intervento medico	2			OM	SIL 1	SIL 2	> 1 g. – < = 2 sett.	4	Possibile	3	Impos
Reversibile, pronto soccorso	1				OM	SIL 1	> 2 sett. – <= 1 anno	3	Raramente	2	Pos
							> 1 anno	2	Trascurabile	1	Pr

N. serie	N. pericolo	Pericolo	Se	Fr	Pr	Av	Cl	Misura di sicurezza

Commenti

L'uso di ognuno dei due metodi sopra menzionati dovrebbe fornire risultati equivalenti. Ogni metodo traduce dettagliatamente il contenuto dello standard a cui appartiene.

In entrambi i casi, è estremamente importante attenersi alle linee guida contenute nel testo dello standard. Il grafico e la tabella dei rischi non devono essere usati prescindendo dal loro contesto o in modo troppo semplicistico.

Valutazione

Dopo aver scelto la misura di protezione e prima che questa sia implementata, è importante ripetere la stima dei rischi. Questa procedura viene spesso trascurata. È possibile che, installando una misura di protezione, l'operatore alla macchina si senta totalmente e completamente protetto contro il rischio originale previsto. Non avendo più la consapevolezza del pericolo originale, può interagire con la macchina in modo diverso, esponendosi più frequentemente al rischio, o ad esempio introducendosi eccessivamente nella macchina. Ciò significa che, se la misura di protezione non funziona, l'operatore sarà esposto a un rischio superiore rispetto a quello inizialmente calcolato. Questo è il rischio effettivo che deve essere stimato. Pertanto, la stima del rischio deve essere ripetuta considerando ogni prevedibile modifica delle modalità di interazione tra l'uomo e la macchina. Il risultato di questa attività serve a controllare che le misure di protezione proposte siano, di fatto, adeguate. Per ulteriori informazioni, si rimanda all'Allegato A di IEC 62061.

Formazione, dispositivi di protezione personale, ecc.

È importante che gli operatori ricevano l'addestramento necessario relativo ai metodi di lavoro sicuri per una specifica macchina. Questo non significa che le altre misure possano esser omesse. Non è accettabile limitarsi a dire all'operatore che non deve avvicinarsi alle aree pericolose invece di installare le adeguate protezioni.

Può anche essere necessario che l'operatore usi dispositivi quali guanti speciali, occhiali, respiratori, ecc. Il progettista della macchina dovrebbe specificare i tipi di dispositivi necessari. L'uso di dispositivi di protezione personale non rappresenta il metodo di sicurezza primario, ma completa le misure di cui sopra.

Standard

Sono diversi gli standard e i rapporti tecnici che forniscono consigli sulla valutazione dei rischi. Alcuni sono di ampia applicabilità mentre altri riguardano applicazioni specifiche.

Quella che segue è una lista di standard che includono informazioni sulla valutazione dei rischi.

ANSI B11.TR3: Risk assessment and risk reduction – A guide to estimate, evaluate and reduce risks associated with machine tools.

ANSI PMMI B155.1: Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery.

ANSI RIA R15.06: Safety Requirements for Industrial Robots and Robot Systems.

AS 4024.1301-2006: Principles of risk assessment.

CSA Z432-04: Safeguarding of Machinery.

CSA Z432-03: Industrial Robots and Robot Systems – General Safety Requirements.

IEC/EN 61508: Functional safety of electrical, electronic and programmable electronic safety-related systems.

IEC/EN 62061: Functional safety of safety related electrical, electronic and programmable electronic control systems.

ISO 14121 (EN 1050): Principles for risk assessment.

Misure di protezione e dispositivi complementari

Quando la valutazione del rischio evidenzia che una macchina o un processo implicano un rischio di lesione personale, tale rischio deve essere eliminato o contenuto. Il modo in cui questo obiettivo viene raggiunto dipende dalla natura della macchina e del pericolo. I dispositivi di protezione sono strumenti che impediscono o rilevano l'accesso a un pericolo. Tra questi, ci sono protezioni fisse, protezioni interbloccate, barriere fotoelettriche, pedane di sicurezza, comandi a due mani e interruttori di abilitazione.

Protezioni fisse che impediscono l'accesso

Se il pericolo riguarda una parte della macchina a cui non è necessario accedere, questa dovrebbe essere protetta mediante una protezione fissa. Per rimuovere questo tipo di protezioni, dovrebbe essere necessario utilizzare degli utensili. Le protezioni fisse devono essere in grado di 1) far fronte all'ambiente operativo, 2) contenere eventuali pezzi scagliati con violenza e 3) non creare pericoli evitando, ad esempio, la presenza di bordi taglienti. Le protezioni fisse possono essere dotate di aperture in corrispondenza del punto di unione con la macchina o per l'utilizzo di recinzioni a rete metallica.

Le finestre rappresentano un efficiente mezzo per monitorare le macchine per l'accesso alla parte specifica della macchina. Occorre prestare attenzione alla selezione dei materiali usati, poiché le interazioni chimiche con fluidi di taglio e i raggi ultravioletti o il semplice invecchiamento ne provocano l'usura nel tempo.

La dimensione delle aperture deve impedire che l'operatore possa essere esposto al pericolo. La tabella O-10 di OSHA 1910.217 (f) (4), ISO 13854, la tabella D-1 di ANSI B11.19, la tabella 3 di CSA Z432 e AS4024.1 forniscono istruzioni sulla distanza necessaria tra l'apertura e la fonte di pericolo.

Rilevamento degli accessi

Per rilevare l'accesso al pericolo, si utilizza un dispositivo di protezione. Quando si sceglie il rilevamento come metodo di riduzione dei rischi, il progettista deve essere consapevole della necessità di un completo sistema di sicurezza; il dispositivo di sicurezza, da solo, non fornisce la necessaria riduzione dei rischi.

Questo sistema di sicurezza, generalmente, è costituito da tre blocchi: 1) un dispositivo di ingresso che rileva l'accesso al pericolo, 2) un dispositivo logico che elabora i segnali provenienti dal dispositivo di rilevamento, controlla lo stato del sistema di sicurezza e attiva o disattiva i dispositivi di uscita, 3) un dispositivo di uscita che controlla l'attuatore (ad es. un motore).

Dispositivi di rilevamento

Per rilevare la presenza di una persona che entra o si trova all'interno di una zona pericolosa, sono disponibili molti dispositivi alternativi. La scelta migliore per una particolare applicazione dipende da una serie di fattori.

- Frequenza di accesso,
- Tempo di arresto del pericolo,
- Importanza del completamento del ciclo della macchina, e
- Contenimento di pezzi scagliati con violenza, fluidi, nebbie, vapori, ecc.

Protezioni mobili, adeguatamente selezionate, possono essere interbloccate per offrire protezione contro pezzi scagliati con violenza, fluidi, nebbie e altri tipi di pericolo; questo tipo di protezione viene spesso utilizzata quando l'accesso al pericolo non è frequente. Le protezioni interbloccate possono anche essere bloccate per impedire l'accesso alla macchina durante il ciclo e quando la macchina impiega molto tempo per fermarsi.

I dispositivi di rilevamento accesso – come barriere fotoelettriche, pedane e scanner – forniscono un rapido e facile accesso alla zona di pericolo e vengono spesso selezionati quando gli operatori devono accedere frequentemente a tale zona. Questo tipo di dispositivi non fornisce protezione contro pezzi scagliati in aria, nebbie, fluidi o altri tipi di pericoli.

La scelta migliore di misura protettiva è un dispositivo o un sistema che garantisca la massima protezione con la minima interferenza nel normale funzionamento della macchina. Tutti gli aspetti della macchina devono essere considerati poiché l'esperienza insegna che si tende a non utilizzare o "aggirare" un sistema difficile da usare.

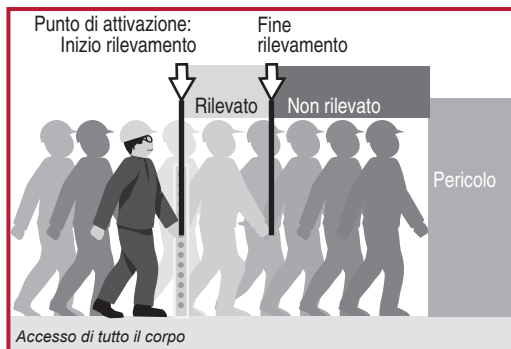
Dispositivi di rilevamento accesso

Quando occorre decidere come proteggere un'area, è importante comprendere a fondo quali funzioni di sicurezza sono necessarie. Di norma, vi saranno almeno due funzioni.

- Disattivare o disabilitare l'alimentazione quando un persona entra nell'area pericolosa.
- Evitare l'attivazione o l'abilitazione dell'alimentazione quando una persona si trova nell'area pericolosa.

A prima vista, potrebbero sembrare una sola funzione, ma sebbene siano strettamente legate e spesso attuate dalla stessa attrezzatura, si tratta di due funzioni separate. Per realizzare la prima funzione occorre disporre di un dispositivo di protezione, ossia un dispositivo che rilevi che una parte del corpo della persona si trova oltre un determinato punto e invii un segnale per disinserire l'alimentazione. Se la persona riesce a oltrepassare il punto di intervento e la sua presenza non è più rilevata, la seconda funzione (evitare il reinserimento dell'alimentazione) non è stata realizzata.

Accesso di tutto il corpo

Accesso parziale del corpo

Lo schema che segue mostra un esempio di accesso di un corpo con un barriera fotoelettrica montata verticalmente che funge da dispositivo di protezione. Anche le porte di protezione interbloccate possono essere considerate come dispositivi di solo intervento quando non c'è niente a impedire che la porta si richiuda dopo l'ingresso.

Se l'accesso dell'intera persona non è possibile, così che una persona non possa proseguire dopo il punto di intervento, la presenza è sempre rilevata e anche la seconda funzione (impedire il reinserimento dell'alimentazione) è attivata.

Per le applicazioni che richiedono un accesso parziale del corpo, gli stessi tipi di dispositivi svolgono la funzione di intervento e di rilevamento accesso. L'unica differenza sta nel tipo di applicazione.

I dispositivi di rilevamento accesso servono a rilevare la presenza di persone. La famiglia di dispositivi include barriere fotoelettriche di sicurezza, barriere di sicurezza a fascio singolo, scanner della zona di sicurezza, pedane e bordi di sicurezza.

Barriere fotoelettriche di sicurezza

Le barriere fotoelettriche di sicurezza possono essere descritte semplicemente come sensori di presenza fotoelettrici concepiti specificatamente per proteggere il personale dai movimenti pericolosi delle macchine. Note anche come AOPD (dispositivi di protezione optoelettrici attivi) o ESPE (dispositivi elettrosensibili di protezione), le barriere fotoelettriche garantiscono un livello di sicurezza ottimale, pur consentendo un'elevata produttività. Sono inoltre soluzioni più ergonomiche rispetto alle protezioni meccaniche. Sono perfette per le applicazioni in cui il personale necessita di accedere frequentemente e facilmente a un punto di lavoro pericoloso.

Le barriere fotoelettriche sono concepite e testate per rispondere a IEC 61496-1 e -2. L'Allegato IV della Direttiva Macchine Europea ne richiede la certificazione da parte di organismi terzi, prima della commercializzazione nella Comunità Europea. Gli organismi terzi testano le barriere fotoelettriche per verificarne la conformità a questo standard internazionale. Underwriter's Laboratory ha adottato IEC 61496-1 come standard nazionale USA.

Laser scanner di sicurezza

I laser scanner di sicurezza sono dotati di uno specchio rotante che deflette gli impulsi luminosi su un arco, creando un piano di rilevamento. La posizione dell'oggetto è determinata dall'angolo di rotazione dello specchio. Usando la tecnica "time-of-flight" (tempo di volo) di un raggio riflesso di luce invisibile, lo scanner può rilevare anche la distanza dell'oggetto dallo scanner stesso. Considerando la distanza misurata e la posizione dell'oggetto, il laser scanner ne determina la posizione esatta.

Pedane di sicurezza sensibili alla pressione

Questi dispositivi servono a proteggere un'area a pavimento intorno alla macchina. Una matrice di pedane interconnesse viene disposta intorno all'area pericolosa e qualsiasi pressione esercitata sulla pedana (ad esempio il passo di un operatore) farà sì che l'unità di controllo della pedana tolga alimentazione alla fonte di pericolo. Le pedane sensibili alla pressione sono spesso usate nell'ambito di un'area recintata contenente diverse macchine, ad esempio nelle celle automatizzate flessibili di produzione o a robot. Quando è necessario accedere alla cella (ad es. per operazioni di regolazione o per "istruire" un robot), le pedane impediscono movimenti pericolosi se l'operatore si allontana dalla zona sicura o deve recarsi dietro a una parte dell'apparecchiatura.

Le dimensioni e il posizionamento della pedana devono considerare la distanza di sicurezza.

Bordi sensibili alla pressione

Questi dispositivi sono strisce di bordatura flessibili che possono essere montate sui margini di una parte in movimento, ad esempio un piano macchina o una porta automatica, che potrebbero schiacciare o ferire gli operatori.

Se la parte in movimento urta l'operatore (o viceversa), il bordo sensibile flessibile viene premuto, comandando l'interruzione dell'alimentazione del componente pericoloso. I bordi sensibili possono inoltre essere usati per proteggere le macchine che potrebbero intrappolare l'operatore. Se un operatore resta intrappolato nella macchina, il contatto con il bordo sensibile provocherà lo spegnimento dell'alimentazione.

Per la realizzazione dei bordi di sicurezza, sono disponibili diverse tecnologie. Una tecnologia molto diffusa è l'inserimento di un lungo interruttore all'interno del bordo. Questo approccio consente di avere bordi dritti e, generalmente, usa la tecnica di collegamento a 4 fili.

Barriere fotoelettriche, scanner, pedane e bordi sensibili sono classificati come "dispositivi di protezione". In effetti non impediscono l'accesso, semplicemente si attivano quando lo rilevano, segnalandolo. La capacità di garantire la sicurezza dipende interamente dalla loro capacità di rilevamento e di interruzione. In generale, sono adatti solo a macchine che si arrestano in tempi ragionevolmente rapidi dopo l'interruzione dell'alimentazione. Poiché un operatore può camminare o raggiungere direttamente l'area pericolosa, è ovviamente necessario che il tempo

richiesto per l'interruzione del movimento sia minore di quello necessario affinché l'operatore raggiunga l'area pericolosa dopo aver azionato il dispositivo di protezione.

Consultare www.ab.com/safety per ulteriori informazioni sul rilevamento degli accessi.

Interruttori di sicurezza

Quando l'accesso alla macchina non è frequente, è preferibile ricorrere a protezioni mobili (apribili). La protezione è interbloccata con l'alimentazione della fonte di pericolo in modo che, quando la porta di protezione non è chiusa, l'alimentazione sia disinserita. Questo metodo implica l'uso di un interruttore di interblocco fissato alla porta di protezione. Il controllo dell'alimentazione della fonte di pericolo è collegato alla sezione dell'interruttore dell'unità. L'alimentazione è generalmente elettrica, ma può anche essere pneumatica o idraulica. Quando il movimento della porta di protezione (apertura) è rilevato, l'interruttore di interblocco comanda l'isolamento dell'alimentazione direttamente o tramite un contattore (o valvola).

Alcuni interruttori di interblocco comprendono anche un dispositivo di blocco che blocca in posizione chiusa la porta della protezione e non viene rilasciato finché la macchina non si trova in una condizione sicura. Per la maggior parte delle applicazioni, la combinazione di protezione mobile e interruttore di interblocco con o senza blocco della protezione è la soluzione più affidabile ed efficiente.

È disponibile un'ampia serie di interruttori di sicurezza, tra cui i seguenti.

- **Interruttori di interblocco con attuatore** – il funzionamento di questi dispositivi richiede l'inserimento e la rimozione dell'attuatore nell'interruttore.
- **Interruttori di interblocco a cerniera** – questi dispositivi sono situati sulle cerniere delle porte di protezione e funzionano utilizzando l'azione di apertura della porta.
- **Interruttori con blocco della protezione** – in alcune applicazioni, è necessario bloccare la porta in chiusura o temporizzarne l'apertura. I dispositivi adatti a questa funzione sono gli interruttori con blocco della protezione. Sono adatti a macchine con caratteristiche di arresto progressivo, ma possono fornire un importante potenziamento della sicurezza per la maggior parte delle macchine.
- **Interruttori di interblocco senza contatto** – questi dispositivi non richiedono alcun contatto fisico per l'attivazione e alcune versioni integrano una funzione di codifica che incrementa il livello di protezione dalle manomissioni.
- **Interblocchi di posizione (interruttori di finecorsa)** – i commutatori a camme sono, di solito, interruttori di finecorsa (o di posizione) a modalità positiva con camma lineare o rotante. Si utilizzano, generalmente, sulle protezioni scorrevoli.
- **Interblocchi a chiave bloccata codificata –** Le chiavi bloccate codificate possono servire all'interblocco del comando o dell'alimentazione. Nel caso di "interblocco del

comando", un dispositivo di interblocco invia un comando di arresto a un dispositivo intermedio che, a sua volta, disattiva un successivo dispositivo per scollegare l'alimentazione dall'attuatore. Nel caso di "interblocco dell'alimentazione", il comando di arresto interrompe direttamente l'alimentazione agli attuatori della macchina.

Dispositivi di interfaccia operatore

Funzione di arresto – Negli Stati Uniti, in Canada, in Europa e a livello internazionale, esiste l'armonizzazione degli standard per quanto riguarda le descrizioni delle categorie di arresto delle macchine o degli impianti di produzione.

NOTA: tali categorie sono diverse da quelle previste da EN 954-1 (ISO 13849-1). Vedere gli standard NFPA79 e IEC/EN 60204-1 per ulteriori informazioni. Gli arresti sono suddivisi in tre categorie.

Categoria 0 arresto dovuto all'immediato scollegamento dell'alimentazione degli attuatori della macchina. Sono considerati arresti non controllati. Con l'alimentazione disinserita, l'azione di frenata, che richiede energia, non sarà attiva. Questo consente ai motori di girare liberamente e rallentare fino a fermarsi dopo un certo periodo di tempo. In altri casi, è possibile che i sistemi di fissaggio della macchina depositino del materiale e che l'alimentazione sia necessaria per tenere fermo tale materiale. I sistemi di arresto meccanici, poiché non richiedono alimentazione, possono essere usati anche con un arresto di categoria 0. L'arresto di categoria 0 ha la priorità sugli arresti di categoria 1 o 2.

Categoria 1 arresto comandato in cui l'alimentazione è disponibile affinché gli attuatori della macchina eseguano l'arresto. Quindi, l'alimentazione viene rimossa dagli attuatori dopo l'arresto. Questa categoria di arresti consente una frenata con alimentazione che provoca l'arresto rapido del movimento pericoloso, successivamente l'alimentazione può essere rimossa dagli attuatori.

Categoria 2 arresto comandato con alimentazione disponibile per gli attuatori della macchina. Un normale arresto di produzione è considerato un arresto di categoria 2.

Queste categorie di arresti devono essere applicate a ciascuna funzione di arresto; nel caso in cui per funzione di arresto si intende l'azione intrapresa dalle parti correlate alla sicurezza del sistema di controllo come reazione a un ingresso, deve essere usata la categoria 0 o 1. Le funzioni di arresto devono avere la precedenza sulle funzioni di avviamento. La scelta della categoria di arresto per ogni funzione di arresto deve essere determinata mediante valutazione dei rischi.

Funzione di arresto d'emergenza

La funzione di arresto d'emergenza deve operare come un arresto di categoria 0 o 1, a seconda di quanto determinato dalla valutazione del rischio. Deve essere avviata da un'unica azione umana. Quando viene eseguita, deve avere la precedenza su tutte le altre funzioni e modalità di funzionamento della macchina. L'obiettivo è quello di togliere alimentazione il più rapidamente possibile senza creare rischi aggiuntivi.

Fino a poco tempo fa erano necessari componenti elettromeccanici cablati per i circuiti di arresto di emergenza. Grazie alle recenti modifiche apportate a standard come IEC 60204-1 e NFPA 79, nei circuiti di arresto di emergenza possono essere utilizzati PLC di sicurezza e altre forme di logica elettronica rispondenti ai requisiti di standard come IEC 61508.

Dispositivi di arresto di emergenza

Laddove sussiste il pericolo che un operatore sia messo a rischio da una macchina, occorre che l'accesso al dispositivo di arresto d'emergenza sia facile. Il dispositivo di arresto di emergenza deve essere costantemente in funzione e facilmente disponibile. I pannelli operatore dovrebbero contenere almeno un dispositivo di arresto d'emergenza. È possibile utilizzare ulteriori dispositivi di arresto d'emergenza in altre posizioni, se necessario. I dispositivi di arresto d'emergenza hanno varie forme. Gli intrruttori con pulsante e gli interruttori a fune sono esempi dei dispositivi più comunemente diffusi. Quando viene azionato, il dispositivo di arresto di emergenza deve rimanere in posizione premuta e non deve essere possibile generare il comando di arresto senza tale condizione. Il reset del dispositivo di arresto di emergenza non deve creare una situazione pericolosa. Deve inoltre essere eseguita un'azione separata e deliberata per riavviare la macchina.

Per ulteriori informazioni sui dispositivi di arresto d'emergenza, vedere ISO/EN 13850, IEC 60947-5-5, NFPA79 e IEC 60204-1, AS4024.1, Z432-94.

Pulsanti di arresto d'emergenza

I dispositivi di arresto di emergenza sono considerati apparecchiature di protezione complementari. Poiché non impediscono e non rilevano l'accesso a un pericolo, non sono considerati dispositivi di protezione primari.

Il tipo più comune di questo tipo di dispositivi sono i pulsanti rossi a fungo posti su sfondo giallo che l'operatore preme in caso di emergenza (vedere la figura 4.59). Devono essere distribuiti strategicamente e in quantità sufficiente intorno alla macchina per garantire che ve ne sia sempre uno a portata di mano nell'area pericolosa.

I pulsanti di arresto di emergenza devono essere immediatamente accessibili e disponibili in tutte le modalità di funzionamento della macchina. I pulsanti utilizzati come dispositivi di arresto di emergenza devono essere a fungo (o azionabili con il palmo della mano) e di colore rosso su sfondo giallo. Quando il pulsante viene premuto, i contatti devono cambiare stato non appena il pulsante si blocca in posizione premuta.

Una delle tecnologie più recenti per gli arresti di emergenza è una tecnica di automonitoraggio. Alla parte posteriore dell'arresto di emergenza, viene aggiunto un contatto addizionale che monitora se i componenti del pannello sono presenti. Questo sistema è il cosiddetto blocco di contatti ad autosorveglianza. Consiste in un contatto, azionato a molla, che si chiude quando il blocco di contatti viene inserito in posizione sul pannello. La Figura 4.60 mostra il contatto di autosorveglianza collegato in serie a uno dei contatti di sicurezza ad apertura diretta.

Interruttori a fune

Per le macchine quali i nastri trasportatori, spesso è più comodo ed efficace usare un dispositivo a fune posto lungo l'area di pericolo (come mostrato nella Figura 4.61.) come dispositivo di arresto d'emergenza. Questi dispositivi usano un cavo d'acciaio collegato all'interruttore di blocco a fune in modo tale che tirando il cavo in qualsiasi punto lungo la sua lunghezza l'interruttore venga attivato e interrompa l'alimentazione della macchina.

Gli interruttori a fune devono rilevare sia il tensionamento sul cavo che l'eventuale mancanza di tensionamento. Quest'ultima funzione assicura che il cavo non sia tagliato e, quindi, pronto all'uso.

La distanza del cavo incide sulle prestazioni dell'interruttore. Per brevi distanze, a una estremità è installato l'interruttore di sicurezza e, all'altra estremità, una molla di tensione. Per lunghe distanze, l'interruttore di sicurezza deve essere installato a entrambe le estremità del cavo, in modo da garantire che una singola azione dell'operatore generi un comando di arresto. La forza di trazione necessaria non dovrebbe superare i 200 N o una distanza di 400 mm nel punto centrale tra i due supporti del cavo.

Comandi a due mani

L'uso dei comandi a due mani (chiamati anche comandi bimanuali) è un metodo molto diffuso per evitare l'accesso a una macchina mentre questa si trova in una condizione pericolosa. Per avviare la macchina, occorre azionare contemporaneamente due comandi (entro 0,5 s uno dall'altro). In questo modo, entrambe le mani dell'operatore sono impegnate in una posizione sicura (ossia sui comandi) e non possono quindi essere spostate nell'area pericolosa. I comandi devono essere azionati continuamente finché permane una situazione di pericolo. Quando uno dei comandi viene rilasciato, il funzionamento della macchina deve cessare e, prima che la macchina possa essere riavviata, devono essere rilasciati entrambi i comandi.

Un sistema di controllo a due mani dipende fortemente dalla capacità del sistema di monitoraggio e di controllo di rilevare eventuali guasti, dunque è importante che questo aspetto sia progettato con le specifiche corrette. La prestazione del sistema di sicurezza a due mani è classificata in Tipi da ISO 13851 (EN 574), correlati alle Categorie ISO 13849-1. I tipi più comunemente usati per la sicurezza delle macchine sono IIIB e IIIC. La tabella che segue mostra la relazione tra i tipi e le categorie di sicurezza.

Requisiti	Tipi				
	I	II	III		
			A	B	C
Attivazione sincrona			X	X	X
Uso della Categoria 1 (da ISO 13849-1)	X		X		
Uso della Categoria 3 (da ISO 13849-1)		X		X	
Uso della Categoria 4 (da ISO 13849-1)					X

La progettazione fisica degli spazi deve impedire l'uso improprio (ad es. utilizzando una mano e un gomito). Ciò è possibile mediante un calcolo delle distanze o l'installazione di schermi. La macchina non deve passare da un ciclo a un altro senza il rilascio e la pressione di entrambi i pulsanti. Questo evita la possibilità che entrambi i pulsanti siano bloccati, lasciando così la macchina in continuo funzionamento. Il rilascio di uno qualsiasi dei pulsanti deve provocare l'arresto della macchina.

L'uso del controllo a due mani deve essere analizzato con attenzione poiché in genere lascia comunque un certo margine di rischio. Il comando a due mani protegge solo la persona che lo usa. L'operatore protetto deve essere in grado di osservare tutta l'area di accesso al pericolo, poiché le altre persone potrebbero non essere protette.

ISO 13851 (EN 574) fornisce ulteriori informazioni sul comando a due mani.

Dispositivi di abilitazione

I dispositivi di abilitazione sono controlli che permettono a un operatore di entrare in una zona pericolosa solo premendo e tenendo premuto l'interruttore di abilitazione. I dispositivi di abilitazione sono dotati di interruttori a due o tre posizioni. I tipi a due posizioni sono disattivati quando l'attuatore non è premuto e attivati in caso contrario. Gli interruttori a tre posizioni sono disattivati quando non premuti (posizione 1), attivati quando tenuti in posizione centrale (posizione 2) e disattivati quando premuti oltre la posizione centrale (posizione 3). Inoltre, nel ritorno dalla posizione 3 alla posizione 1, il circuito di uscita non deve chiudersi passando attraverso la posizione 2.

I dispositivi di abilitazione devono essere usati in combinazione con altre funzioni di sicurezza. Un tipico esempio è il controllo del movimento in modalità lenta. Dopo aver attivato la modalità lenta, l'operatore può entrare nella zona di pericolo con il dispositivo di abilitazione.

Quando si usa un dispositivo di abilitazione, un segnale deve indicare che il dispositivo di abilitazione è attivo.

Dispositivi logici

I dispositivi logici svolgono un ruolo centrale tra i componenti di sicurezza del sistema di controllo. I dispositivi logici effettuano il controllo e il monitoraggio del sistema di sicurezza e consentono l'avviamento della macchina o eseguono i comandi per il suo arresto.

Per creare un'architettura di sicurezza rispondente alla complessità e alla funzionalità di ogni macchina, è disponibile un'ampia serie di dispositivi logici. I piccoli relè di monitoraggio di sicurezza cablati sono più economici e quindi adatti alle macchine più piccole in cui, per completare la funzione di sicurezza, è necessario un dispositivo logico dedicato. I relè di sicurezza di monitoraggio modulari e configurabili sono preferibili dove è necessario un maggior numero di dispositivi di protezione e un controllo di zona minimo. Le macchine medio/grandi e più complesse devono invece considerare sistemi programmabili con I/O distribuiti.

Relè di monitoraggio di sicurezza

I moduli relè di monitoraggio di sicurezza (MSR) svolgono un ruolo centrale in molti sistemi di sicurezza. Questi moduli sono generalmente costituiti da due o più relè a guida forzata con circuiteria addizionale per garantire le prestazioni della funzione di sicurezza.

I relè a guida forzata sono relè specializzati “ice-cube”. I relè a guida forzata devono rispondere ai requisiti prestazionali di EN 50025. Fondamentalmente, sono concepiti per evitare che contatti normalmente chiusi e normalmente aperti si chiudano simultaneamente. Concezioni più recenti sostituiscono le uscite elettromeccaniche con uscite di sicurezza allo stato solido.

I relè di monitoraggio di sicurezza realizzano diversi controlli sul sistema di sicurezza. All'accensione, effettuano l'autodiagnostica sui propri componenti interni. Quando i dispositivi di ingresso sono attivati, il relè MSR confronta i risultati degli ingressi ridondanti. Se accettabili, l'MSR controlla gli attuatori esterni. Se il risultato è positivo, l'MSR attende un segnale di reset per eccitare le sue uscite.

La selezione del relè di sicurezza più adatto dipende da una serie di fattori: il tipo di dispositivo che deve monitorare, il tipo di reset, il numero e il tipo di uscite.

Tipi di ingressi

I dispositivi di protezione hanno diversi modi di indicare il verificarsi di un evento:

Interblocchi a contatto e pulsanti di emergenza: contatti meccanici, a singolo canale con un contatto normalmente chiuso o a doppio canale con entrambi i contatti normalmente chiusi. L'MSR deve essere in grado di accettare il singolo o il doppio canale e garantire il rilevamento dei guasti incrociati per la configurazione a due canali.

Interblocchi senza contatto e pulsanti di emergenza: contatti meccanici a doppio canale, uno normalmente aperto e uno normalmente chiuso. L'MSR deve essere in grado di elaborare diversi ingressi.

Dispositivi di commutazione uscite allo stato solido: barriere fotoelettriche, laser scanner, dispositivi senza contatto allo stato solido hanno due uscite sourcing ed effettuano il rilevamento dei propri guasti incrociati. L'MSR deve essere in grado di ignorare il metodo di rilevamento dei guasti incrociati dei dispositivi.

Pedane sensibili alla pressione: le pedane creano un cortocircuito tra due canali. L'MSR deve essere in grado di sopportare cortocircuiti ripetuti.

Bordi sensibili alla pressione: alcuni bordi sono concepiti come pedane a 4 fili. Alcuni sono dotati di dispositivi a due fili che creano una variazione della resistenza. L'MSR deve essere in grado di rilevare un cortocircuito o la variazione della resistenza.

Tensione: misura la forza contro-elettromotrice di un motore durante la decelerazione. L'MSR deve essere in grado di tollerare alte tensioni e di rilevare basse tensioni quando il motore rallenta.

Arresto del movimento: l'MSR deve rilevare i treni di impulsi da diversi sensori ridondanti.

Dispositivo di comando a due mani: l'MSR deve rilevare ingressi diversi, normalmente aperti e normalmente chiusi, oltre a fornire la temporizzazione di 0,5 s e la logica sequenziale.

I relè di monitoraggio di sicurezza devono essere concepiti specificamente per interfacciare ognuno di questi dispositivi, poiché hanno diverse caratteristiche elettriche. Alcuni MSR possono collegarsi a diversi tipi di ingressi ma, una volta scelto il dispositivo, l'MSR si può interfacciare solo con quel dispositivo. Il progettista deve selezionare un MSR che sia compatibile con il dispositivo di ingresso.

Impedenza d'ingresso

L'impedenza d'ingresso dei relè di sicurezza di monitoraggio determina il numero di dispositivi d'ingresso che possono essere connessi al relè e fino a che distanza essi possono essere montati. Ad esempio, un relè di sicurezza può avere un'impedenza consentita massima di 500 Ohm. Quando l'impedenza d'ingresso è superiore a 500 Ohm, le uscite non vengono attivate. L'utente deve prestare particolare attenzione per garantire che l'impedenza d'ingresso rimanga al di sotto della massima della specifica. La lunghezza, la dimensione e il tipo di cavo usato incidono sull'impedenza d'ingresso.

Numero di dispositivi di ingresso

Il processo di valutazione del rischio deve essere usato per determinare il numero di dispositivi di ingresso da collegare a un relè di monitoraggio di sicurezza (MSR) e la frequenza con cui tali dispositivi devono essere controllati. Per garantire che gli arresti d'emergenza e gli interblocchi della porta siano funzionanti, devono essere controllati a intervalli regolari, in base a quanto determinato dalla valutazione del rischio. Ad esempio, un MSR di ingresso a canale doppio collegato a una porta interbloccata che deve essere aperta a ogni ciclo della macchina (ad esempio più volte al giorno) potrebbe non dover essere controllato. Questo accade perché l'apertura della protezione fa sì che l'MSR stesso controlli i propri ingressi e uscite (in funzione della configurazione) per verificare la presenza di singoli guasti. Più di frequente viene aperta la protezione, maggiore è l'integrità del processo di verifica.

Un altro esempio sono gli arresti di emergenza. Poiché tali arresti sono generalmente usati solo per le emergenze, è probabile che siano usati raramente. Occorre dunque stabilire un programma che verifichi gli arresti di emergenza e ne confermi l'efficienza a intervalli pianificati. Questo modo di verificare il sistema di sicurezza è conosciuto come "test funzionale" e il tempo tra le verifiche è chiamato "intervallo tra test funzionali". Un terzo esempio potrebbero essere le porte di accesso per la regolazione delle macchine che, come i pulsanti di arresto di emergenza, vengono utilizzate raramente. Anche in questo caso, dovrebbe essere stabilito un programma per verificarne la funzionalità a intervalli programmati.

La valutazione del rischio aiuta a determinare se i dispositivi di ingresso devono essere controllati e con quale frequenza. Più alto è il livello del rischio, maggiore è l'integrità richiesta al processo di verifica. Minore è la frequenza del comando "automatico", maggiore deve essere la frequenza della verifica "manuale" imposta.

Rilevamento dei guasti incrociati dei dispositivi di ingresso

Nei sistemi a due canali, il sistema di sicurezza deve rilevare i guasti di cortocircuito tra canali dei dispositivi di ingresso, chiamati anche guasti incrociati. Questo avviene tramite il dispositivo di rilevamento o il relè di monitoraggio di sicurezza.

I relè di monitoraggio di sicurezza a microprocessore – come barriere fotoelettriche, laser scanner e sensori avanzati senza contatto – rilevano questi cortocircuiti in molti modi. Un modo comune di rilevare i guasti incrociati è il test con impulsi diversi. Gli impulsi dei segnali di uscita sono molto rapidi. L'impulso del canale 1 è sfasato rispetto a quello del canale 2. Se si verifica un corto, gli impulsi sono simultanei e vengono rilevati dal dispositivo.

I relè di monitoraggio di sicurezza elettromeccanici usano un'altra tecnica di differenziazione: un ingresso pull-up e un ingresso pull-down. Un corto dal canale 1 al canale 2 attiva il dispositivo di protezione dalle sovracorrenti e il sistema di sicurezza procede allo spegnimento.

Uscite

Gli MSR sono disponibili con più uscite. I tipi di uscite aiutano a determinare quale MSR usare in determinate applicazioni.

Molti MSR hanno almeno 2 uscite di sicurezza immediatamente operative. Le uscite di sicurezza MSR sono normalmente aperte. Sono considerate di sicurezza grazie alla ridondanza e al controllo interno. Un secondo tipo di uscita sono le uscite temporizzate. Le uscite temporizzate vengono generalmente usate negli arresti di Categoria 1, in cui la macchina ha bisogno di tempo per l'arresto prima di permettere l'accesso alla zona pericolosa. Gli MSR hanno anche uscite ausiliarie. Generalmente, si tratta di uscite normalmente chiuse.

Caratteristiche delle uscite

Le caratteristiche delle uscite descrivono la capacità del dispositivo di protezione di commutare carichi. Generalmente, le caratteristiche dei dispositivi industriali sono descritte come resistive o elettromagnetiche. Un carico resistivo può essere un elemento riscaldatore. I carichi elettromagnetici sono generalmente relè, contattori o solenoidi che hanno una forte caratteristica induttiva del carico. L'allegato A dello standard IEC 60947-5-1 descrive le categorie dei carichi. Le categorie sono riportate anche nella sezione 'Principi' del catalogo di sicurezza.

Lettera di designazione: è una lettera seguita da un numero, ad esempio A300. La lettera fa riferimento alla corrente termica convenzionale in custodia e se la corrente è continua o alternata. Ad esempio, A rappresenta 10 amp di corrente alternata. Il numero sta per la tensione di isolamento nominale. Ad esempio, 300 significa 300 V.

Utilizzo: l'utilizzo descrive i tipi di carichi per la cui commutazione il dispositivo è progettato. Gli utilizzi pertinenti allo standard IEC 60947-5 sono riportati nella tabella che segue.

Utilizzo	Descrizione del carico
AC-12	Controllo di carichi resistivi e carichi a stato solido con optoaccoppiatori di isolamento
AC-13	Controllo di carichi a stato solido con trasformatore d'isolamento
AC-14	Controllo di piccoli carichi elettromagnetici (meno di 72 VA)
AC-15	Carichi elettromagnetici superiori a 72 VA
DC-12	Controllo di carichi resistivi e carichi a stato solido con fotoaccoppiatori di isolamento
DC-13	Controllo di elettromagneti
DC-14	Controllo di carichi elettromagnetici con resistori nel circuito

Corrente termica, Ith: la corrente termica convenzionale in custodia è il valore della corrente usata per i test di aumento della temperatura dell'apparecchiatura, quando è montata in una custodia specificata.

Tensione operativa Ue e corrente Ie nominali: i valori nominali di corrente e tensione di funzionamento indicano la capacità di chiusura e apertura degli elementi di commutazione in condizioni operative normali. I prodotti Allen-Bradley Guardmaster hanno valori nominali specifici di 125 V CA, 250 V CA e 24 V CC. Consultare il produttore per informazioni sull'uso a tensioni diverse da quelle specificate.

VA: i valori VA (Tensione x Amperaggio) indicano i valori nominali degli elementi di commutazione quando si chiude o si apre il circuito.

Esempio 1: un valore di A150, AC-15 indica che i contatti possono chiudere un circuito di 7200 VA. A 120 V CA, i contatti possono chiudere un circuito con una corrente di spunto di 60 A. Poiché l'AC-15 è un carico elettromagnetico, i 60 amp avranno solo una durata limitata, la corrente di spunto del carico elettromagnetico. L'apertura del circuito è a soli 720 VA poiché la corrente a regime del carico elettromagnetico è pari a 6 A, ossia la corrente nominale di funzionamento.

Esempio 2: un valore nominale di N150, DC-13 indica che i contatti possono chiudere un circuito di 275 VA. A 125 V CA, i contatti possono chiudere un circuito con un picco di 2,2 amp. I carichi elettromagnetici in CC non hanno correnti di spunto come quelli in CA. L'apertura del circuito è dunque a 275 VA perché la corrente a regime del carico elettromagnetico è pari a 2,2, la corrente nominale di funzionamento.

Riavviamento della macchina

Se, ad esempio, una protezione interbloccata viene aperta su una macchina in funzione, l'interruttore di interblocco di sicurezza arresta la macchina. Nella maggior parte delle circostanze, è essenziale che la macchina non si riavvii immediatamente dopo la chiusura della protezione. Uno dei modi più comuni per ottenere questo risultato è affidarsi a un contattore di avviamento a ritenuta.

La pressione e il rilascio del pulsante di avvio eccita momentaneamente la bobina di controllo del contattore che chiude i contatti di alimentazione. Finché l'alimentazione è presente tra i contatti, la bobina di controllo rimane eccitata (a ritenuta elettrica) tramite i contatti ausiliari del contattore, accoppiati meccanicamente ai contatti dell'alimentazione. Qualsiasi interruzione dell'alimentazione principale o di controllo ha come risultato la diseccitazione della bobina e l'apertura dei contatti dell'alimentazione principale e ausiliaria. L'interblocco della protezione è cablato nel circuito di controllo del contattore. Questo significa che il riavvio può essere effettuato solo chiudendo la protezione e quindi impostando su "ON" il normale pulsante di avviamento, resettando così il contattore e avviando la macchina.

I requisiti per le normali situazioni di interblocco sono definiti dallo standard ISO 12100-1 Paragrafo 3.22.4 (estratto)

"Quando la protezione è chiusa, le funzioni pericolose della macchina coperte dalla protezione possono operare grazie ad essa, ma la sola chiusura della protezione non attiva il loro funzionamento".

Molte macchine sono già dotate di contattori singoli o doppi che funzionano nel modo descritto precedentemente (o hanno un sistema che ottiene lo stesso risultato). Quando si monta un interblocco su una macchina esistente è necessario determinare se il sistema di controllo dell'alimentazione risponde a tali requisiti e, se necessario, attuare ulteriori misure.

Funzioni di reset

I relè di monitoraggio di sicurezza Allen Bradley Guardmaster sono dotati di reset manuale monitorato o reset automatico/manuale.

Reset manuale monitorato

Un reset manuale monitorato richiede la chiusura e l'apertura di un circuito dopo che la porta è stata chiusa o l'arresto di emergenza resettato. I contatti ausiliari normalmente chiusi ad accoppiamento meccanico dei contattori di commutazione di potenza sono connessi in serie con un pulsante instabile. Una volta che la protezione è stata aperta e chiusa nuovamente, il relè di sicurezza non consente alla macchina di essere riavviata finché il pulsante di reset non è stato premuto e rilasciato. A questo punto, il relè di sicurezza controlla che entrambi i contattori siano su OFF e che entrambi i circuiti di interblocco (e quindi le protezioni) siano chiusi. Se questi controlli sono soddisfacenti, la macchina può essere riavviata con i normali comandi. L'interruttore di reset deve essere posizionato in un luogo che consenta di vedere

bene il pericolo, in modo che l'operatore possa controllare che non presenti più rischi prima di utilizzare la macchina.

Reset automatico/manuale

Alcuni relè di sicurezza sono dotati di reset automatico/manuale. La modalità di reset manuale non è monitorata e il reset avviene quando il pulsante è premuto. Un cortocircuito o un blocco nel pulsante di reset non sarà rilevato. In alternativa, la linea di reset può essere collegata con un ponticello, consentendo un reset automatico. L'utente deve quindi fornire un altro meccanismo per evitare l'avviamento della macchina quando la porta si chiude.

Un dispositivo di reset automatico non richiede un'azione di commutazione manuale, ma dopo la disattivazione condurrà sempre un controllo di integrità del sistema prima di resettare il sistema. Un sistema di reset automatico non deve essere confuso con un dispositivo senza sistemi di reset. In questi, infatti, il sistema di sicurezza sarà attivato immediatamente dopo la disattivazione, ma non sarà effettuato alcun controllo di integrità del sistema.

Protezioni di controllo

Una protezione di controllo arresta una macchina quando la protezione è aperta e l'avvia direttamente quando è chiusa. L'uso di questo tipo di protezioni è consentito solo in determinate condizioni molto precise, poiché qualsiasi avviamento imprevisto o il mancato arresto sarebbero estremamente pericolosi. Il sistema di interblocco deve avere la maggiore affidabilità possibile (spesso è consigliabile usare il blocco elettronico). L'uso delle protezioni di controllo può essere preso in considerazione SOLO per le macchine in cui non esiste ALCUNA POSSIBILITÀ che un operatore o parte del suo corpo si trovino all'interno o raggiungano la zona pericolosa mentre la protezione è chiusa. Inoltre, la protezione di controllo deve costituire l'unico accesso all'area pericolosa.

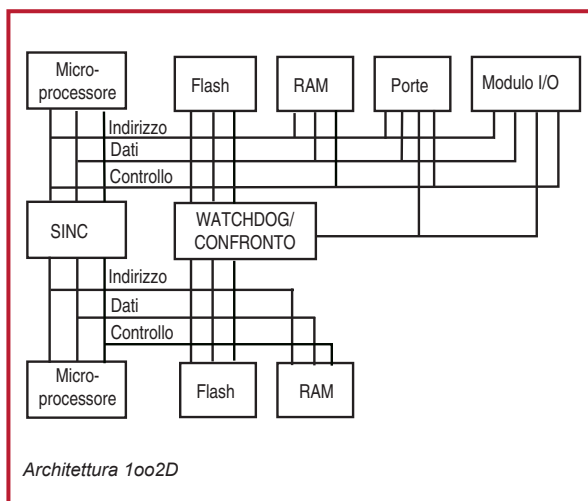
Controlli a logica programmabile di sicurezza

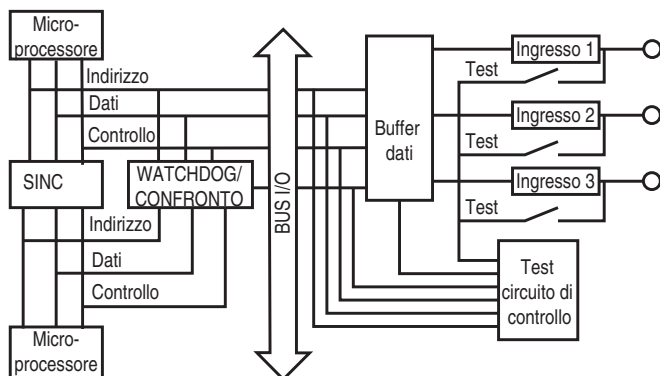
L'esigenza di applicazioni di sicurezza flessibili e scalabili è alla base dello sviluppo dei controllori/PLC di sicurezza. I controllori programmabili di sicurezza offrono agli utilizzatori, in un'applicazione di sicurezza lo stesso livello di flessibilità del controllo che avrebbero con controllori programmabili standard. Tuttavia, le differenze tra PLC standard e di sicurezza sono molte. I PLC di sicurezza sono disponibili in varie piattaforme, per rispondere ai requisiti di scalabilità, funzionalità e integrazione dei più complessi sistemi di sicurezza.

Hardware

Ridondanza delle CPU, memoria, circuiti I/O e diagnostica interna sono funzionalità dei PLC di sicurezza che i PLC standard non hanno. Un PLC di sicurezza dedica molto più tempo alla diagnostica interna su memoria, comunicazioni e I/O. Queste operazioni aggiuntive sono indispensabili a raggiungere la certificazione di sicurezza necessaria. Il sistema operativo del controllore gestisce la ridondanza e la diagnostica addizionale, in modo assolutamente trasparente per il programmatore che può quindi procedere alla programmazione dei PLC di sicurezza quasi come farebbe per i PLC standard.

I microprocessori che controllano questi dispositivi effettuano un'esaustiva diagnostica interna per garantire l'operatività della funzione di sicurezza. Lo schema a blocchi che segue offre un esempio di PLC di sicurezza. Anche se i controllori a microprocessore differiscono leggermente da una famiglia all'altra, i principi applicati per ottenere la classificazione di sicurezza sono simili.

Architettura 1oo2D

Sono molti i microprocessori utilizzati per elaborare I/O, memoria e comunicazioni sicure. Le analisi diagnostiche vengono realizzate da circuiti watchdog. Questo tipo di struttura è nota come 1oo2D, perché uno qualunque dei due microprocessori può realizzare la funzione di sicurezza mentre, nel contempo, una attenta diagnostica garantisce che entrambi i microprocessori stiano funzionando in sincronizzazione.

Inoltre, ogni circuito di ingresso è testato internamente diverse volte al secondo, per verificarne il corretto funzionamento. Grazie a questi continui test, ad esempio, anche se un pulsante di emergenza è premuto una sola volta al mese, il circuito sarà in grado di comunicare correttamente con il PLC di sicurezza.

Schema a blocchi del modulo di ingressi di sicurezza

Le uscite del PLC di sicurezza sono elettromeccaniche o di sicurezza allo stato solido. Come i circuiti di ingresso, anche i circuiti di uscita sono testati diverse volte al secondo per verificare che possano disattivare le uscite. L'uscita che non dovesse rispondere correttamente viene disattivata dalle altre due e il guasto è riportato dal circuito di monitoraggio interno.

Quando si usano dispositivi di sicurezza con contatti meccanici (pulsanti di emergenza, interruttori di porta, ecc.), l'utilizzatore può applicare segnali di prova a impulsi per rilevare i guasti incrociati. Per limitare i costi legati alle uscite di sicurezza, molti PLC di sicurezza sono dotati di specifiche uscite a impulsi che possono essere collegate a dispositivi a contatto meccanico.

Software

La programmazione dei PLC di sicurezza è molto simile a quella dei PLC standard. Il sistema operativo gestisce la diagnostica aggiuntiva e il controllo degli errori, in modo che tale compito non spetti al programmatore. Per molti PLC di sicurezza, sono utilizzate speciali istruzioni di scrittura del programma per il sistema di sicurezza e queste istruzioni tendono a replicare la funzione dei relè di sicurezza. Ad esempio, l'istruzione per il pulsante di emergenza funziona in modo molto simile a un MSR 127. Anche se la logica dietro ognuna di queste istruzioni è complessa, i programmi di sicurezza sembrano relativamente semplici perché il programmatore non fa altro che collegare tra di loro questi blocchi. Queste istruzioni, insieme ad altre istruzioni logiche, matematiche, di manipolazione dati, ecc. sono certificate da terzi per assicurare che il loro funzionamento sia coerente con gli standard applicabili.

I blocchi funzione sono il metodo predominante di programmazione delle funzioni di sicurezza. Oltre ai blocchi funzione e alla logica ladder, i PLC di sicurezza forniscono anche istruzioni applicative di sicurezza certificate. Le istruzioni di sicurezza certificate servono a gestire applicazioni specifiche. Questo esempio mostra una istruzione di arresto di emergenza. Per compiere la stessa funzione in logica ladder sarebbero necessari circa 16 rami di logica ladder.

Poiché il comportamento logico è integrato nell'istruzione per l'arresto di emergenza, la logica integrata non deve essere testata.

I blocchi funzione certificati possono interfacciare quasi tutti i dispositivi di sicurezza. Un'eccezione è data dal bordo di sicurezza a tecnologia resistiva.

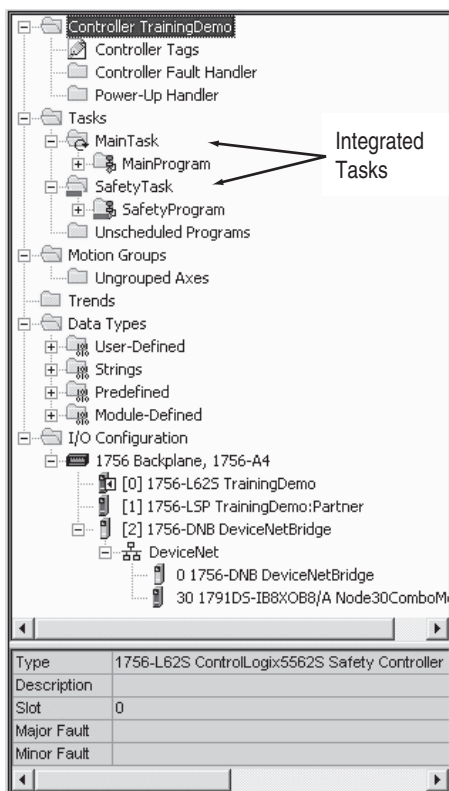
I PLC di sicurezza generano una "firma" che consente di tracciare le eventuali modifiche apportate. Questa firma è di solito una combinazione di programma, configurazione ingressi/uscite e registrazione cronologica. Quando il programma è terminato e convalidato, l'utente dovrebbe registrare questa firma tra i risultati di convalida, per futuro riferimento. Se il programma ha bisogno di modifiche, è richiesta una nuova convalida e la registrazione di una nuova firma. Per impedire modifiche non autorizzate, il programma può anche essere bloccato con una password.

Il cablaggio dei sistemi a logica programmabile è semplificato rispetto a quello dei relè di monitoraggio di sicurezza. Anziché essere cablati a terminali specifici dei relè di monitoraggio di sicurezza, i dispositivi di ingresso sono collegati a qualunque terminale di ingresso e i dispositivi di uscita a qualunque terminale di uscita. I terminali sono poi assegnati mediante software.

Controllori di sicurezza integrati

Attualmente, le soluzioni di controllo di sicurezza offrono la completa integrazione in una singola architettura di controllo, in cui le funzioni di controllo di sicurezza e quelle standard risiedono e lavorano insieme. La capacità di realizzare task di movimento, azionamento, processo, batch, sequenziali ad alta velocità e sicurezza SIL 3 in un controllore offre notevoli vantaggi. L'integrazione di controllo standard e di sicurezza consente di utilizzare strumenti e tecnologie comuni che riducono i costi associati a progettazione, installazione, messa in servizio e manutenzione. La possibilità di utilizzare, sulle reti di sicurezza, hardware di controllo, dispositivi o I/O di sicurezza distribuiti e dispositivi di interfaccia operatore comuni riduce i costi di acquisto e manutenzione, oltre ai tempi di sviluppo. Tutte queste funzioni aumentano la produttività e la velocità della ricerca guasti e favoriscono la riduzione dei costi di formazione.

Lo schema che segue mostra un esempio dell'integrazione di controllo e sicurezza. Le funzioni di controllo non legate alla sicurezza standard risiedono nel Main Task. Le funzioni di controllo legate alla sicurezza risiedono nel Safety Task.

Tutte le funzioni standard e di sicurezza sono isolate una dall'altra. Ad esempio, i tag di sicurezza possono essere letti direttamente dalla logica standard. I tag di sicurezza possono essere scambiati tra i controllori GuardLogix su EtherNet, ControlNet o DeviceNet. I dati dei tag di sicurezza possono essere letti direttamente da dispositivi esterni, interfacce operatore (HMI), personal computer (PC) o altri controllori.

1. Logica e tag standard si comportano come ControlLogix.

2. Dati tag standard, analizzati dal programma o dal controllore e dispositivi esterni, interfacce operatore, PC, altri controllori, ecc.

3. Come un controllore integrato, GuardLogix permette di trasferire (mappare) dati tag standard nei tag di sicurezza da usare per task di sicurezza. Per gli utilizzatori, ciò significa poter leggere informazioni di stato sul lato standard di GuardLogix. I dati non devono essere usati per controllare direttamente una uscita di sicurezza.

4. I tag di sicurezza possono essere letti direttamente dalla logica standard.

5. I tag di sicurezza possono essere letti o scritti dalla logica di sicurezza.

6. I tag di sicurezza possono essere scambiati tra i controllori GuardLogix su EtherNet.

7. I dati tag di sicurezza, analizzati dal programma o dal controllore, possono essere letti da dispositivi esterni, interfacce operatore, PC, altri controllori, ecc. Dopo essere stati letti, questi dati sono considerati dati standard, non di sicurezza.

Reti di sicurezza

Le reti di comunicazione a livello di impianto hanno permesso ai fabbricanti di migliorare la flessibilità, aumentare le capacità di diagnostica e le distanze, ridurre i costi di installazione e cablaggio, facilitare la manutenibilità e, in generale, migliorare la produttività delle loro operazioni di produzione. Le stesse motivazioni sono alla base dell'implementazione delle reti di sicurezza industriali. Queste reti di sicurezza consentono ai fabbricanti di distribuire I/O e dispositivi di sicurezza sui macchinari mediante un semplice cavo di rete, riducendo i costi di installazione, migliorando la diagnostica e installando sistemi di sicurezza di maggiore complessità. Permettono, inoltre, la comunicazione sicura tra PLC e controllori di sicurezza, dando agli utilizzatori la possibilità di distribuire il controllo di sicurezza tra diversi sistemi intelligenti.

Le reti di sicurezza non impediscono l'occorrenza di errori di comunicazione. Le reti di sicurezza hanno una maggiore capacità di rilevamento degli errori di trasmissione per cui, successivamente, i dispositivi di sicurezza adottano le misure adeguate. Tra gli errori di comunicazione rilevati, ci sono i seguenti: inserimento di messaggi, perdita di messaggi, corruzione di messaggi, ritardo di messaggi, ripetizione di messaggi e sequenza non corretta dei messaggi.

Per molte applicazioni, quando viene rilevato un errore, il dispositivo entra in uno stato di diseccitazione, tipicamente chiamato "stato di sicurezza." Il dispositivo di ingresso o di uscita di sicurezza deve rilevare questi errori di comunicazione e poi entrare, se necessario, in stato di sicurezza.

Le prime reti di sicurezza erano legate a un particolare tipo di supporto o schema di accesso ai supporti e, di conseguenza, i fabbricanti dovevano usare cavi, schede di interfaccia di rete, router, ponti, ecc. specifici, che diventavano parte integrante della funzione di sicurezza. Queste reti erano limitate per il fatto che supportavano solo la comunicazione tra i dispositivi di sicurezza. Ciò significava che i fabbricanti dovevano usare due o più reti per la loro strategia di controllo delle macchine (una rete per il controllo standard e un'altra per il controllo di sicurezza), con l'aumento dei costi di installazione, formazione e dei pezzi di ricambio.

Le moderne reti di sicurezza consentono di comunicare con dispositivi di controllo standard e di sicurezza mediante un unico cavo di rete. CIP (Common Industrial Protocol) Safety è un protocollo standard aperto, pubblicato da ODVA (Open DeviceNet Vendors Association), che permette la comunicazione di sicurezza tra i dispositivi di sicurezza su reti DeviceNet, ControlNet e EtherNet/IP. Dato che CIP Safety è una estensione del protocollo CIP standard, i dispositivi di sicurezza e quelli standard possono risiedere tutti sulla stessa rete. Gli utilizzatori possono anche collegare tra loro a ponte reti contenenti dispositivi di sicurezza, con la possibilità di suddividere i dispositivi di sicurezza per regolare con precisione i tempi di risposta o, semplicemente, per facilitare la distribuzione dei dispositivi di sicurezza. Dato che il protocollo di sicurezza è di esclusiva responsabilità dei dispositivi finali (PLC di sicurezza/controllori, moduli I/O di sicurezza, componenti di sicurezza), tutti i componenti quali cavi, schede di interfaccia di rete, ponti e router sono standard e quindi esclusi dalla funzione di sicurezza oltre a non richiedere hardware di rete specifico.

Dispositivi di uscita

Contattori e relè di controllo di sicurezza

Contattori e relè di controllo servono a togliere alimentazione all'attuatore. Per la classificazione di sicurezza, contattori e relè di controllo sono dotati di funzioni speciali.

Per il feedback sullo stato dei contattori e dei relè di controllo al dispositivo logico, si utilizzano contatti normalmente chiusi ad accoppiamento meccanico. L'uso di contatti ad accoppiamento meccanico aiuta a garantire la funzione di sicurezza. Per rispondere ai requisiti dei contatti ad accoppiamento meccanico, i contatti normalmente chiusi e quelli normalmente aperti non possono essere, contemporaneamente, in stato di chiusura. IEC 60947-5-1 definisce i requisiti per i contatti ad accoppiamento meccanico. Se i contatti normalmente aperti si saldano, i contatti normalmente chiusi rimangono aperti di almeno 0,5 mm. Viceversa, se i contatti normalmente chiusi si saldano, i contatti normalmente aperti rimangono aperti.

I sistemi di sicurezza devono essere avviati solo in posizioni specifiche. I contattori e i relè di controllo standard permettono di premere l'indotto per chiudere i contatti normalmente aperti. Sui dispositivi di sicurezza, l'indotto è protetto dall'override manuale per ridurre il rischio di avviamento non intenzionale.

Sui relè di controllo di sicurezza, il contatto normalmente chiuso è azionato dal comando principale. I contattori di sicurezza usano un blocco per contatti supplementare per posizionare i contatti ad accoppiamento meccanico. Se il blocco di contatti fuoriesce dalla base, i contatti ad accoppiamento meccanico rimangono chiusi. I contatti ad accoppiamento meccanico sono fissati permanentemente al relè di controllo o al contattore di sicurezza.

Sui contattori più grandi, un blocco per contatti supplementare è insufficiente a riflettere accuratamente lo stato dell'azionamento più grande. Su entrambi i lati del contattore, sono situati dei contatti speculari (Figura 4.81).

Il tempo di diseccitazione dei relè di controllo o dei contattori influisce sul calcolo della distanza di sicurezza. Spesso, nella bobina, è installato un soppressore di picchi di tensione che aumenta la vita dei contatti che azionano la bobina. Per le bobine CA, il tempo di diseccitazione rimane invariato. Per le bobine CC, il tempo di diseccitazione aumenta. L'aumento dipende dal tipo di soppressione selezionato.

Contattori e relè di controllo sono concepiti per commutare grandi carichi, da 0,5 A a oltre 100 A. Il sistema di sicurezza funziona a basse correnti. Il segnale di feedback generato dal dispositivo logico del sistema di sicurezza può andare da pochi milliampere a decine di milliampere, di solito a 24 VCC. Per commutare in modo affidabile una corrente così bassa, contattori e relè di controllo di sicurezza sono dotati di contatti biforcati, placcati in oro.

Protezione dai sovraccarichi

Gli standard elettrici impongono la protezione dei motori dai sovraccarichi. La diagnostica fornita dal dispositivo di protezione dai sovraccarichi aumenta non solo la sicurezza dell'apparecchiatura ma anche quella dell'operatore. Le tecnologie attualmente disponibili possono rilevare condizioni di guasto come sovraccarico, mancanza di fase, guasto verso terra, stallo, blocco, sottocarico, squilibrio di corrente e sovratemperatura. Il rilevamento e la comunicazione delle condizioni anomale prima dell'intervento aiutano a ridurre i tempi di fermo della produzione e a proteggere operatori e personale di manutenzione da condizioni di pericolo impreviste.

Azionamenti e asservimenti

Azionamenti e asservimenti di sicurezza possono essere usati per impedire la trasmissione dell'energia rotazionale e permettere un arresto di sicurezza o un arresto di emergenza.

Gli inverter ottengono la classificazione di sicurezza con canali ridondanti per togliere alimentazione dalla circuiteria del controllo di gate. Un canale è il segnale di abilitazione, un segnale hardware che rimuove il segnale di ingresso alla circuiteria del controllo di gate. Il secondo canale è un relè a guida forzata che scollega l'alimentazione elettrica dalla circuiteria del controllo di gate. Il relè a guida forzata, inoltre, ritrasmette un segnale di stato al sistema logico. Questo approccio ridondante consente di applicare l'azionamento di sicurezza ai circuiti di arresto di emergenza, senza bisogno di un contattore.

L'asservimento funziona in modo simile agli inverter, mediante segnali di sicurezza ridondanti per ottenere la funzione di sicurezza. Un segnale interrompe il comando alla circuiteria del controllo di gate. Un secondo segnale scollega l'alimentazione elettrica dalla circuiteria del controllo di gate. Due relè a guida forzata sono utilizzati per rimuovere i segnali e fornire feedback al dispositivo logico di sicurezza.

Sistemi di collegamento

I sistemi di collegamento aggiungono valore riducendo i costi di installazione e manutenzione dei sistemi di sicurezza. I progetti devono prendere in considerazione sistemi a canale singolo, a doppio canale, a doppio canale con segnalazione e molteplici tipi di dispositivi.

Quando è necessario un collegamento in serie di interblocchi a due canali, un blocco di distribuzione può semplificare l'installazione. Con un grado di protezione IP67, questi dispositivi possono essere installati sulla macchina in posizioni remote. Quando è necessario un diverso gruppo di dispositivi, è possibile utilizzare un modulo ArmorBlock Guard I/O. Per installare vari tipi di dispositivi, gli ingressi possono essere configurati via software.

Calcolo delle distanze di sicurezza

Le funzioni di sicurezza devono intervenire in tempo per evitare che l'operatore possa raggiungere il punto di pericolo. Per il calcolo delle distanze di sicurezza, esistono due gruppi di standard. In questo capitolo, questi standard sono raggruppati come segue:

ISO EN: (ISO 13855 ed EN 999)

US CAN (ANSI B11.19, ANSI RIA R15.06 e CAN/CSA Z434-03)

Formula

La distanza minima di sicurezza dipende dal tempo necessario a elaborare il comando di arresto e da quanto l'operatore può penetrare la zona di rilevamento prima del rilevamento. In tutto il mondo, la formula utilizzata ha la stessa forma e gli stessi requisiti. Le differenze sono i simboli usati per rappresentare variabili e unità di misura.

Le formule sono:

ISO EN:	S =	K x	T	+ C
US CAN:	Ds =	K x	(Ts + Tc + Tr + Tbm)	+ Dpf

Dove: Ds e S sono la distanza di sicurezza minima dalla zona di pericolo al più vicino punto di rilevamento

Direzioni di avvicinamento

Quando si considera il calcolo della distanza di sicurezza per una barriera fotoelettrica o uno scanner, occorre considerare l'avvicinamento al dispositivo di rilevamento. L'avvicinamento può essere di tre tipi:

Normale – avvicinamento perpendicolare al piano di rilevamento

Orizzontale – avvicinamento parallelo al piano di rilevamento

Inclinato – avvicinamento inclinato rispetto alla zona di rilevamento.

Costante di velocità

K è una costante di velocità. Il valore della costante di velocità dipende dai movimenti dell'operatore (velocità delle mani, velocità di camminata e lunghezza del passo). Questo parametro è basato su dati di ricerca secondo cui è ragionevole presumere, per il movimento della mano di un operatore a corpo fermo, una velocità di 1600 mm/sec. Occorre comunque considerare le circostanze effettive dell'applicazione. In linea generale, la velocità di avvicinamento varierà da 1600 mm/s a 2500 mm/sec. La costante di velocità adeguata deve essere determinata mediante la valutazione dei rischi.

Tempo di arresto

T è il tempo di arresto globale del sistema. Il tempo totale, in secondi, inizia dalla generazione del segnale di arresto alla cessazione del pericolo. Per facilitare l'analisi, questo tempo può essere suddiviso nelle sue parti incrementali (Ts, Tc, Tr e Tbm). Ts è il tempo di arresto peggiore della macchina/apparecchiatura. Tc è il tempo di arresto peggiore del sistema di controllo. Tr è il tempo di risposta del dispositivo di protezione, compresa la sua interfaccia. Tbm è l'ulteriore tempo di arresto consentito dal dispositivo di controllo del freno prima che rilevi il superamento dei limiti predeterminati dall'utente finale per il tempo di decelerazione. Tbm si usa con presse meccaniche a tavola rotante. Ts + Tc + Tr sono usualmente misurati da un dispositivo di misurazione del tempo di arresto se i valori sono sconosciuti.

Fattori di penetrazione in profondità

I fattori di penetrazione in profondità sono rappresentati dai simboli C e Dpf. Si tratta della corsa massima verso il pericolo prima del rilevamento da parte del dispositivo di protezione. I fattori di penetrazione in profondità cambiano a seconda del tipo di dispositivo e di applicazione. Per determinare il miglior fattore di penetrazione in profondità, occorre far riferimento allo standard corrispondente. Per un normale avvicinamento a una barriera fotoelettrica o a uno scanner, la cui sensibilità agli oggetti è inferiore a 64 mm, gli standard ANSI e canadesi usano:

Dpf = 3,4 x (Sensibilità oggetti – 6,875 mm), ma non meno di zero.

Per un normale avvicinamento a una barriera fotoelettrica o a uno scanner, la cui sensibilità agli oggetti è inferiore a 40 mm, gli standard ISO e EN usano:

C = 8 x (Sensibilità oggetti – 14 mm), ma non meno di 0

Queste due formule hanno un punto di convergenza a 19,3 mm. Per sensibilità agli oggetti inferiori a 19 mm, lo standard US CAN è più restrittivo, dato che la barriera fotoelettrica o lo scanner dell'area devono essere maggiormente allontanate dal pericolo. Per sensibilità agli oggetti superiori a 19,3 mm, è più restrittivo lo standard ISO EN. I costruttori che intendono commercializzare le loro macchine in tutto il mondo devono prevedere le condizioni peggiori di entrambe le equazioni.

Applicazioni “reach-through” (attraversamento)

Quando si utilizzano sensibilità agli oggetti più grandi, gli standard US CAN e ISO EN differiscono leggermente sul fattore di penetrazione in profondità e sulla sensibilità agli oggetti. La figura 5.2 riepiloga le differenze. Il valore ISO EN è di 850 mm mentre il valore US CAN è 900 mm. Gli standard differiscono anche nella sensibilità agli oggetti. Lo standard ISO EN ammette valori compresi tra 40 e 70 mm, mentre lo standard US CAN ammette fino a 600 mm.

Applicazioni “reach-over” (superamento)

Entrambi gli standard concordano che l’altezza minima del raggio più basso dovrebbe essere di 300 mm, ma differiscono per quanto riguarda l’altezza minima del raggio più alto. ISO EN stabilisce 900 mm, mentre US CAN stabilisce 1200 mm. Il valore per il raggio più alto sembra essere controverso. Quando si considera una applicazione “reach-through”, l’altezza del raggio più alto dovrà essere molto più elevata per un operatore in posizione eretta. Se l’operatore può oltrepassare la parte superiore del piano di rilevamento, allora si applica il criterio “reach-over”.

Raggi singoli o multipli

I raggi separati, singoli o multipli, sono ulteriormente definiti negli standard ISO EN. Le figure che seguono mostrano le altezze “praticabili” dei raggi multipli rispetto al pavimento. La penetrazione in profondità è di 850 mm per la maggior parte dei casi e di 1200 mm per il raggio singolo. In confronto, lo standard US CAN considera ciò tra i requisiti “reach-through”. Il passaggio sopra, sotto o attorno ai raggi singoli o multipli deve sempre essere preso in considerazione.

Numero di raggi	Altezza dal pavimento (mm)	C (mm)
1	750	1200
2	400, 900	850
3	300, 700, 1100	850
4	300, 600, 900, 1200	850

Calcoli della distanza

Per il normale avvicinamento alla barriera fotoelettrica, il calcolo della distanza di sicurezza, per ISO EN e US CAN, è simile ma esistono delle differenze. Per il normale avvicinamento a barriere fotoelettriche verticali la cui sensibilità agli oggetti è di 40 m max., lo standard ISO EN richiede due fasi. Innanzitutto, calcolare S usando 2000 come costante di velocità.

S = 2000 x T + 8 x (d -1 4)

La distanza minima per S è di 100 mm.

Una seconda fase può essere usata quando la distanza è superiore a 500 mm. Il valore di K può essere ridotto a 1600. Quando si usa K = 1600, il valore minimo di S è 500 mm.

Lo standard US CAN usa l'approccio a una fase: Ds = 1600 x T * Dpf

Ciò comporta differenze superiori al 5% tra gli standard, quando il tempo di risposta è inferiore a 560 ms.

Avvicinamenti inclinati

La maggior parte delle applicazioni con barriera fotoelettrica e scanner sono installate in verticale (avvicinamento normale) o in orizzontale (avvicinamento parallelo). Questi montaggi non sono considerati inclinati se l'angolazione è compresa tra ±5° rispetto alla progettazione. Quando l'angolo supera ±5°, occorre prendere in considerazione i rischi potenziali (ad es. distanza più corta) degli avvicinamenti prevedibili. In generale, angoli superiori a 30° rispetto al piano di riferimento (ad es. pavimento) dovrebbero essere considerati normali e quelli inferiori a 30 considerati paralleli.

Pedane di sicurezza

Con le pedane, la distanza di sicurezza deve prendere in considerazione velocità e passo degli operatori. Si presume che l'operatore cammini e che le pedane di sicurezza siano installate a pavimento. Il primo passo dell'operatore sulla pedana ha un fattore di penetrazione in profondità di 1200 mm. Se l'operatore deve salire su una piattaforma, il fattore di penetrazione in profondità può essere ridotto del 40% per l'altezza del passo.

Esempio

Esempio: un operatore si avvicina normalmente a una barriera fotoelettrica di 14 mm, collegata a un relè di monitoraggio di sicurezza che, a sua volta, è collegato a un contattore CC con un soppressore a diodi. Il tempo di risposta del sistema di sicurezza, Tr, è 20 + 15 + 95 = 130 ms. Il tempo di arresto della macchina, Ts+Tc, è 170 ms. Il dispositivo di controllo del freno non è utilizzato. Il valore Dpf è 1 pollice e il valore C è zero. Il calcolo sarebbe il seguente:

Dpf = 3,4 (14 – 6,875) = 1 poll. (24,2 mm)

Ds = K x (Ts + Tc + Tr + Tbm) + Dpf
Ds = 63 x (0,17 + 0,13 + 0) + 1
Ds = 63 x (0,3) + 1
Ds = 18,9 + 1
Ds = 19,9 in (505 mm)

C = 8 (14-14) = 0

S = K x T + C
S = 1600 x (0,3) + 0
S = 480 mm (18,9 in)

Quindi, per una macchina utilizzabile in qualunque parte del mondo, la distanza di sicurezza minima a cui la barriera fotoelettrica di sicurezza deve essere montata rispetto al pericolo è di 20 pollici o 508 mm.

Prevenzione dell'accensione non intenzionale

La prevenzione dell'accensione non intenzionale è coperta da molti standard, tra cui ISO 14118, EN 1037, ISO 12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 e AS 4024.1603. Questi standard hanno un oggetto comune: il metodo primario per impedire accensioni non intenzionali è scollegare l'alimentazione al sistema e bloccare il sistema in stato di disattivazione. Lo scopo è permettere alle persone di entrare in sicurezza nelle zone pericolose della macchina.

Lockout/Tagout

Le macchine nuove devono essere costruite con dispositivi di isolamento dell'alimentazione bloccabili. I dispositivi si applicano a tutti i tipi di energia – elettrica, idraulica, pneumatica, gravitazionale e laser. Per lockout si intende l'applicazione di un blocco a un dispositivo di isolamento dell'alimentazione. Il blocco deve essere rimosso solo dal suo proprietario o da un supervisore, in condizioni controllate. Quando sulla macchina devono lavorare diverse persone, ogni persona deve applicare il proprio blocco ai dispositivi di isolamento dell'alimentazione. Ogni blocco deve essere rapportabile al suo proprietario.

Negli USA, il tagout è una alternativa al lockout per le macchine più vecchie su cui non è mai stato installato un dispositivo lucchettabile. In questo caso, la macchina viene spenta e viene applicato un cartellino per avvisare tutto il personale di non avviare la macchina mentre l'operatore che ha apposto il cartellino sta lavorando sulla macchina. A partire dal 1990, le macchine che sono state modificate devono essere aggiornate in modo da prevedere un dispositivo lucchettabile di isolamento dell'alimentazione.

Un dispositivo di isolamento dell'alimentazione è un dispositivo meccanico che, fisicamente, impedisce la trasmissione o il rilascio di energia. Questi dispositivi possono essere interruttori automatici, sezionatori, interruttori manuali, combinazioni spina/presa o valvole manuali. I dispositivi di isolamento elettrico devono commutare tutti i conduttori di alimentazione non messi a terra e nessun polo può operare in modo indipendente.

Lo scopo del lockout e del tagout è impedire l'avviamento non intenzionale della macchina. L'avviamento non intenzionale può essere il risultato di varie cause: un guasto del sistema di controllo, un'azione inadeguata su un comando di avviamento, un sensore, un contattore o una valvola, il ripristino dell'alimentazione dopo un'interruzione o una serie di altre influenze interne o esterne. Al termine del processo di lockout/tagout, deve essere verificata la dissipazione dell'energia.

Sistemi di isolamento di sicurezza

I sistemi di isolamento di sicurezza eseguono lo spegnimento ordinario di una macchina consentendo, nel contempo, di scollegare l'alimentazione in modo semplice. Questo approccio funziona bene con macchine e sistemi di fabbricazione più grandi, soprattutto quando diverse fonti di alimentazione sono situate a livello intermedio o in posizioni distanti.

Sezionatori di carico

Per l'isolamento locale dei dispositivi elettrici, subito a valle del dispositivo da isolare e bloccare possono essere installati degli interruttori. Gli interruttori di carico serie 194E sono un esempio di prodotto in grado sia di isolare sia di bloccare.

Sistemi a chiave bloccata

I sistemi a chiave bloccata sono un altro metodo per implementare un sistema di lockout. Molti sistemi a chiave bloccata sono inizializzati da un dispositivo di isolamento dell'alimentazione. Quando l'interruttore è spento dalla chiave "primaria", l'alimentazione alla macchina viene rimossa, simultaneamente, da tutti i conduttori di alimentazione non messi a terra. La chiave primaria può quindi essere rimossa e portata nel posto in cui è necessario accedere alla macchina. La Figura 6.4 mostra un esempio del sistema più semplice, un sezionatore e un blocco di accesso. Per configurazioni di lockout più complesse, possono essere aggiunti vari componenti.

Misure alternative al lockout

Lockout e tagout devono essere usati durante le operazioni di manutenzione o assistenza sulle macchine. Gli interventi sulla macchina durante le normali operazioni di produzione sono protetti. La differenza tra le operazioni di assistenza/manutenzione e quelle di normale funzionamento non è sempre chiara.

Alcune regolazioni e interventi di assistenza di minore importanza che avvengono durante le normali operazioni di produzione non richiedono necessariamente il lock-out della macchina. Si tratta, ad esempio, di carico e scarico dei materiali, modifiche e regolazioni ordinarie degli utensili, controllo dei livelli di lubrificazione e rimozione del materiale di scarto. Queste attività devono essere di routine, ripetitive e integranti nell'utilizzo dell'apparecchiatura di produzione e il lavoro è realizzato usando misure di protezione alternative che forniscono effettiva protezione. Tra queste misure, ci sono le protezioni interbloccate, le barriere fotoelettriche e le pedane di sicurezza. Usate con adeguati dispositivi di uscita e logici di sicurezza, gli operatori possono accedere in sicurezza alle zone di pericolo della macchina per le normali attività di produzione o di assistenza.

Struttura dei sistemi di controllo legati alla sicurezza

Introduzione

Che cos'è un sistema di controllo legato alla sicurezza (spesso abbreviato SRCS)? Si tratta della parte di un sistema di controllo di una macchina atta a impedire che si verifichi una condizione pericolosa. Può essere un sistema dedicato separato o essere integrato all'interno del normale sistema di controllo della macchina.

La sua complessità va da un sistema semplice, come l'interruttore di interblocco di una porta e l'interruttore per un arresto di emergenza collegati in serie fino alla bobina di controllo di un contattore di potenza o a un sistema composto che comprende sia dispositivi semplici sia complessi, comunicanti attraverso software e hardware.

I sistemi di controllo legati alla sicurezza sono concepiti per realizzare funzioni di sicurezza. Il sistema SRCS deve continuare a funzionare correttamente in tutte le condizioni prevedibili. Quindi che cos'è una funzione di sicurezza, come possiamo progettare un sistema per realizzarla e una volta messa a punto, come dimostrare la sua efficacia?

Funzione di sicurezza

Una funzione di sicurezza è implementata, dai componenti di sicurezza del sistema di controllo della macchina, per ottenere o mantenere l'apparecchiatura in uno stato di sicurezza rispetto a uno specifico pericolo. Un guasto della funzione di sicurezza può comportare un immediato aumento dei rischi legati all'uso dell'apparecchiatura; ovvero una condizione pericolosa.

Una macchina deve presentare almeno un “pericolo”, altrimenti non è una macchina. Una “condizione pericolosa” si verifica quando una persona è esposta a un pericolo. Una condizione pericolosa non implica che la persona sia ferita. La persona esposta può essere in grado di riconoscere il pericolo e di evitare lesioni. La persona esposta può non essere in grado di riconoscere il pericolo o il pericolo può essere originato da un avviamento non intenzionale. Il compito principale del progettista di sistemi di sicurezza è prevenire le condizioni pericolose e gli avviamenti non intenzionali.

La funzione di sicurezza può spesso essere descritta con requisiti multicomponente. Ad esempio, la funzione di sicurezza originata da una protezione di interblocco si basa su tre aspetti:

1. i pericoli coperti dalla protezione non possono agire fino a che la protezione è chiusa;
2. l'apertura della protezione provoca l'arresto del pericolo, se attivo al momento dell'apertura;
3. la chiusura della protezione non riavvia il pericolo coperto dalla protezione.

Quando si definisce la funzione di sicurezza per una specifica applicazione, la parola "pericolo" deve essere sostituita dal pericolo specifico. Il pericolo non deve essere confuso con le sue conseguenze. Schiacciamento, taglio e ustioni sono le conseguenze di un pericolo. Esempi di pericolo sono i motori, stantuffi, coltelli, torce, pompe, laser, robot, organi terminali di robot, solenoidi, valvole, altri tipi di attuatore o pericoli meccanici con effetti gravitazionali.

Nella discussione sui sistemi di sicurezza, è stata utilizzata la frase "in concomitanza o prima della richiesta di intervento della funzione di sicurezza". Che cos'è una richiesta di intervento della funzione di sicurezza? Esempi di richiesta di intervento della funzione di sicurezza sono l'apertura di una protezione interbloccata, l'interruzione di una barriera fotoelettrica, il passo su una pedana di sicurezza o la pressione di un arresto di emergenza. Un operatore chiede che il pericolo sia bloccato o, se questa condizione già sussiste, che non sia trasmessa energia.

I componenti di sicurezza del sistema di controllo della macchina eseguono la funzione di sicurezza. La funzione di sicurezza non è eseguita da un singolo dispositivo, ad esempio, solo dalla protezione. L'interblocco sulla protezione invia un comando a un dispositivo logico che, a sua volta, disabilita un attuatore. La funzione di sicurezza inizia con il comando e finisce con l'implementazione.

Il sistema di sicurezza deve essere progettato con un livello di integrità commisurato ai rischi della macchina. Rischi maggiori richiedono maggiori livelli di integrità per garantire l'operatività della funzione di sicurezza. I sistemi di sicurezza della macchina possono essere categorizzati in base al tipo di progettazione e alla capacità di garantire l'operatività della funzione di sicurezza.

Categorie dei sistemi di controllo

La seguente trattazione delle categorie è basata su ISO 13849-1:1999, equivalente a EN 954-1:1996. Nel 2006, ISO 13849-1 è stata notevolmente rivisto per armonizzarlo con IEC 62061 e IEC 61508 che sono gli standard più utilizzati per i sistemi di sicurezza altamente complessi. La versione 2006 di ISO 13849-1 continua a utilizzare le categorie di prestazione di sicurezza; le categorie sono considerate la "struttura" o "architettura" degli SRCS. Ulteriori informazioni sui componenti e sulla progettazione del sistema, a complemento di questa "struttura", forniscono il "livello prestazionale". La trattazione delle categorie, in questa sede, si applica a entrambe le revisioni 1999 e 2006 di ISO 13849-1.

Lo standard ISO 13849-1 "Safety related parts of control systems, Part 1 General principles for design" è basato su un "linguaggio" di cinque categorie per confrontare e descrivere le prestazioni dei sistemi SRCS.

Nota 1: la categoria B non prevede misure speciali per la sicurezza ma rappresenta la base per le altre categorie.

Nota 2: più errori provocati da una causa comune o inevitabili conseguenze del primo guasto devono essere considerati quale un solo guasto.

Nota 3: la revisione dei guasti può essere limitata a una combinazione di due errori se questo può essere giustificato, ma nel caso di circuiti complessi (ad esempio circuiti a microprocessori) è possibile che sia necessario prendere in considerazione più errori contemporaneamente

Come decidere di quale categoria si ha bisogno? Il processo di valutazione dei rischi dovrebbe condurre alla categoria corretta. Per tradurre questi requisiti nella specifica di un progetto di sistema occorre interpretare i requisiti di base.

Spesso si pensa erroneamente che la categoria 1 fornisca la minore protezione e che la categoria 4 garantisca quella migliore. Questo non è il principio che regola le categorie. Si tratta di punti di riferimento che descrivono le prestazioni funzionali di diversi metodi per garantire la sicurezza dei sistemi di controllo correlati alla sicurezza e dei relativi componenti.

La categoria 1 è volta alla PREVENZIONE degli errori. Si ottiene utilizzando principi progettuali, componenti e materiali adeguati. La semplicità del principio di funzionamento e del progetto, e le caratteristiche stabili e prevedibili del materiale, sono i punti essenziali di questa categoria.

Le categorie 2, 3 e 4 richiedono che se il guasto non può essere prevenuto, deve essere RILEVATO e quindi devono essere presi i provvedimenti necessari.

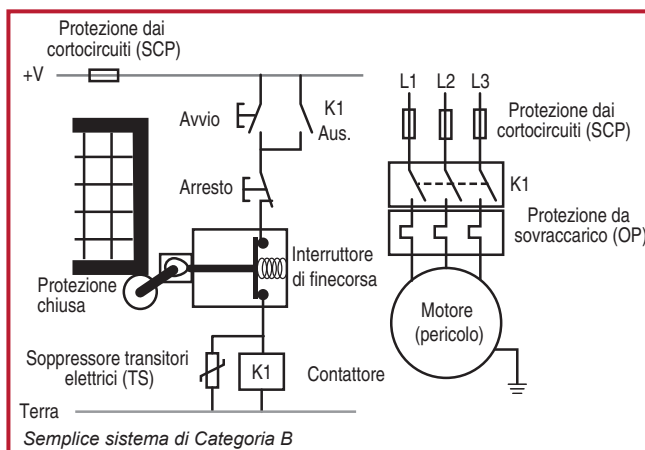
Ridondanza, diversità e monitoraggio sono le chiavi di queste categorie. La ridondanza è la duplicazione della stessa tecnica. La diversità è l’uso di due diverse tecniche. Il monitoraggio è il controllo dello stato dei dispositivi e l’adozione delle misure conseguenti. Il solito (ma non l’unico) metodo di monitoraggio consiste nel replicare le funzioni essenziali per la sicurezza e confrontare il funzionamento.

Riepilogo dei requisiti	Comportamento del sistema
CATEGORIA B (vedere la nota 1) Le parti correlate alla sicurezza del sistema di controllo della macchina e/o l'attrezzatura protettiva, oltre ai relativi componenti, devono essere progettati, costruiti, selezionati, assemblati e combinati in conformità con gli standard pertinenti affinché resistano alle influenze previste. I principi base di sicurezza devono essere applicati.	Quando si verifica un guasto, questo può comportare una perdita della funzione di sicurezza.
CATEGORIA 1 Si applicano i requisiti della categoria B; inoltre occorre usare componenti di sicurezza e principi di sicurezza di comprovata efficienza.	Come per la categoria B ma con una più alta affidabilità della funzione di sicurezza. (Maggiore è l'affidabilità, minore è la probabilità di guasto).
CATEGORIA 2 Si applicano i requisiti della categoria B e principi di sicurezza di comprovata efficienza. Le funzioni di sicurezza devono essere controllate all'avviamento della macchina e periodicamente dal sistema di controllo della macchina. Qualora sia rilevato un guasto deve essere creato uno stato sicuro e, se ciò non fosse possibile, deve essere lanciato un allarme.	La perdita della funzione di sicurezza è rilevata dal controllo. Il verificarsi di un guasto può comportare la perdita della funzione di sicurezza tra gli intervalli di controllo.
CATEGORIA 3 (vedere le note 2 e 3) Si applicano i requisiti della categoria B e principi di sicurezza di comprovata efficienza. Il sistema deve essere progettato in modo che un singolo guasto in una sua parte qualsiasi non comporti la perdita della funzione di sicurezza. Dove possibile, un singolo guasto deve essere rilevato.	Quando si verifica un singolo guasto, la funzione di sicurezza viene sempre eseguita. Alcuni ma non tutti gli errori vengono rilevati. Un accumulo di errori non rilevati può comportare la perdita della funzione di sicurezza.
CATEGORIA 4 (vedere le note 2 e 3) Si applicano i requisiti della categoria B e principi di sicurezza di comprovata efficienza. Il sistema deve essere progettato in modo che un singolo guasto, in qualunque sua parte, non comporti la perdita della funzione di sicurezza. Il singolo guasto deve essere rilevato in occasione o prima della successiva richiesta di intervento della funzione di sicurezza. Se tale rilevamento non è possibile, l'accumulo di errori non deve comportare la perdita della funzione di sicurezza.	Quando si verificano i guasti, la funzione di sicurezza viene sempre eseguita. I guasti vengono rilevati in tempo utile per prevenire la perdita della funzione di sicurezza.

Categoria B

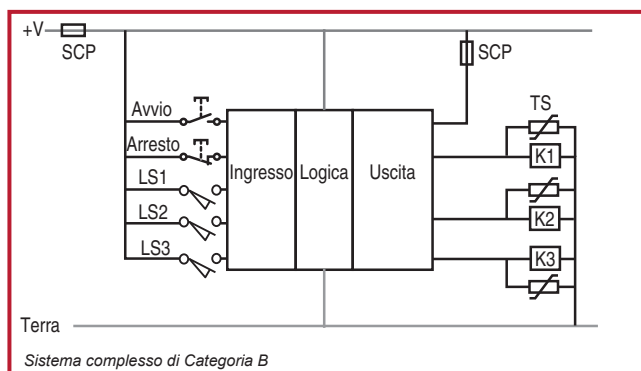
La categoria B fornisce i requisiti di base di qualunque sistema di controllo; che si tratti di un sistema di controllo legato alla sicurezza o meno. Un sistema di controllo deve lavorare nell'ambiente previsto. Il concetto di affidabilità rappresenta un fondamento per i sistemi di controllo, dato che l'affidabilità è definita come la probabilità che un dispositivo realizzi la funzione prevista, per un determinato intervallo, nelle condizioni previste. Anche se abbiamo un sistema che risponde ai nostri obiettivi di affidabilità, sappiamo che il sistema può avere problemi. Il progettista del sistema di sicurezza deve sapere se un guasto del sistema genera un pericolo o non influisce sulle condizioni di sicurezza. Il problema è "Come si comporta il sistema in presenza di guasti?" Iniziando da questo concetto, quali sono i principi da seguire per impostare la progettazione del sistema? La Categoria B richiede l'applicazione dei principi di sicurezza di base. ISO 13849-2 contiene i principi di sicurezza di base dei sistemi elettrici, pneumatici, idraulici e meccanici. I principi elettrici sono riepilogati come segue.

- Corretta selezione, combinazione, disposizione, assemblaggio e installazione (secondo istruzioni mfg'rs)
- Compatibilità dei componenti a tensioni e correnti
- Compatibilità alle condizioni ambientali
- Uso del principio di diseccitazione
- Soppressione dei transitori elettrici
- Riduzione del tempo di risposta
- Protezione contro gli avviamenti non intenzionali
- Fissaggio sicuro dei dispositivi di ingresso (ad es. montaggio di interblocchi)
- Protezione del circuito di controllo (secondo NFPA79 e IEC 60204-1)
- Corretto collegamento equipotenziale di protezione

Semplice sistema di Categoria B

Questo è un esempio di sistema di Categoria B. La protezione è interbloccata con un interruttore di finecorsa a modalità negativa (azionato a molla). Il sistema è protetto contro i cortocircuiti e i sovraccarichi per rispondere ai requisiti elettrici standard di protezione del circuito di controllo. La soppressione dei transitori elettrici serve

a prevenire la saldatura dei contatti quando la bobina del contattore è diseccitata. È stato usato il principio di diseccitazione: l'interblocco di protezione spegne il motore. I componenti devono essere selezionati e installati per adeguarsi alle condizioni ambientali prevedibili e ai requisiti di corrente e tensione. Non è stata applicata alcuna speciale misura di sicurezza di Categoria B e, quindi, potrebbero essere necessarie misure addizionali.

Premere il pulsante di avviamento, con la protezione chiusa, per mettere in tensione il motore, che costituisce il pericolo. Quando il contattore K1 si chiude, un contatto ausiliario mantiene il circuito e il pulsante di avviamento può essere rilasciato. Premere il pulsante di arresto o aprire la protezione per spegnere il motore. Il rilascio del pulsante di arresto o la chiusura della protezione non provocherà il riavviamento del motore.

Sistema complesso di Categoria B

Questo è un sistema complesso che risponde alla Categoria B. Molteplici dispositivi di rilevamento (interruttori di finecorsa) e pulsanti sono collegati al modulo di ingresso di un controllore a logica programmabile (PLC). Molteplici attuatori sono collegati al modulo d'uscita. Un modulo logico, che utilizza software, determina quali uscite attivare o disattivare in risposta allo stato dei dispositivi di rilevamento.

Come facciamo a sapere che questi circuiti rispondono alla Categoria B? Primo, il progettista deve selezionare, installare e assemblare i componenti secondo le istruzioni del fabbricante. Questi dispositivi devono funzionare entro i valori nominali di tensione e corrente previsti. Anche le condizioni ambientali previste devono essere considerate – compatibilità elettromagnetica, vibrazioni, urti, contaminazione, lavaggi. È stato usato il principio di diseccitazione: nelle bobine del contattore, è installata la protezione dai transitori elettrici. Il motore è protetto contro i sovraccarichi. Il cablaggio e la messa a terra rispondono ai corrispondenti standard elettrici.

Il passo successivo, nell'analisi della sicurezza, è la scomposizione del sistema nei suoi principali componenti e l'analisi delle loro modalità di guasto potenziale. In un precedente capitolo, abbiamo visto il sistema suddiviso in tre blocchi, INGRESSO – LOGICA – USCITA. Quando si considerano le prestazioni del sistema di sicurezza, nell'analisi deve essere incluso anche il cablaggio.

Negli esempi della Categoria B, i componenti sono:

- interruttore di interblocco (finecorsa)
- controllore a logica programmabile
- contattore
- cablaggio.

Interruttore di interblocco

L'interruttore di finecorsa è un dispositivo meccanico. L'attività che svolge è semplice: aprire i contatti quando viene aperta la protezione. Molti anni fa, gli interruttori di finecorsa erano usati in questo modo. Ma la loro struttura ha dei limiti che non permettono di giungere a migliori prestazioni di sicurezza. Gli standard elettrici impongono dispositivi di protezione dai cortocircuiti (ad es. fusibili o interruttori automatici) per le linee. Questa protezione può non essere sufficiente a prevenire un contatto saldato nell'interruttore di finecorsa. I contatti nell'interruttore di finecorsa sono concepiti per aprirsi per effetto di una molla. Purtroppo, la forza della molla non è sempre sufficiente a superare la forza di un contatto saldato. Una seconda considerazione è la molla stessa. La ripetuta flessione può comportarne la rottura e la forza esercitata sui contatti può non essere sufficiente ad aprire il circuito. Anche altri guasti interni, nella testa o nel collegamento dell'attuatore, possono far sì che i contatti rimangano chiusi quando la protezione è aperta. Un'altra importante considerazione è l'invalidabilità. Quando la protezione è aperta, l'interruttore di finecorsa può essere facilmente invalidato premendo la leva in posizione di attivazione e mantenendola in posizione con nastro, un filo o altri semplici strumenti.

Controllore a logica programmabile

I PLC sono il sistema di controllo privilegiato per le macchine. I dispositivi di ingresso, come gli interblocchi con interruttori di finecorsa, sono collegati a moduli di ingresso. I dispositivi di uscita, come i contattori, sono collegati a moduli di uscita. Il dispositivo logico assegna i dispositivi di ingresso ai corrispondenti dispositivi di uscita nelle condizioni logiche desiderate.

Sebbene la loro affidabilità sia drasticamente migliorata nel tempo, i PLC sono comunque soggetti a usura e a guasti. Il progettista di sistemi di sicurezza deve conoscere i meccanismi dei possibili guasti e sapere se possono generare condizioni pericolose. I PLC hanno due importanti categorie di guasto: hardware e software. I guasti hardware possono avvenire internamente nei moduli di ingresso, di uscita o logici. Questi guasti possono fare in modo che le uscite rimangano attivate, anche se è stato generato un comando di arresto. Anche i guasti software, nel programma applicativo o nel firmware, possono fare in modo che le uscite rimangano attivate anche se è stato generato un comando di arresto.

Contattore

I contattori eccitano gli attuatori della macchina: motori, solenoidi, elementi riscaldanti e altri tipi di attuatori. Le correnti degli attuatori sono alte e alcune correnti di spunto possono essere 10 volte superiori al loro valore a regime. I contattori dovrebbero sempre prevedere la protezione dei loro contatti elettrici dai sovraccarichi e dai cortocircuiti, per prevenire la saldatura del contatti. Ma anche con questa protezione, i contatti potrebbero rimanere chiusi. Ciò può essere dovuto a saldatura o all'incollamento dell'indotto. Quando si verifica un guasto di questo tipo, il pulsante di arresto diventa inefficace e la macchina deve essere messa fuori tensione mediante il sezionatore principale. I contattori dovrebbero essere regolarmente ispezionati per rilevare eventuali collegamenti allentati che possono provocare surriscaldamento e deformazione. Il contattore deve rispondere agli standard che coprono le caratteristiche e le condizioni d'uso richieste. IEC 60947-4-1 e IEC 60947-5-1 descrivono in modo dettagliato i test a cui devono essere sottoposti i contattori nelle varie applicazioni.

Cablaggio

Anche se progettare e installare nel rispetto del corrispondente standard elettrico riduce la possibilità di guasti di cablaggio, questi possono comunque verificarsi. I guasti di cablaggio da considerare includono cortocircuiti e circuiti aperti. L'analisi dei cortocircuiti deve tener conto di cortocircuiti verso alimentazione, a massa o verso altri circuiti che possono creare una condizione pericolosa.

Interruttori di avviamento e arresto

Anche gli interruttori di avviamento e arresto devono essere considerati. Se il pulsante di avviamento va in cortocircuito, la macchina ripartirà in modo imprevisto al rilascio del pulsante di arresto o alla chiusura della protezione. Fortunatamente, la protezione deve essere chiusa per avviare il motore. Se la protezione è chiusa, l'accesso al pericolo dovrebbe essere protetto. Un pulsante di arresto guasto o in cortocircuito tra i suoi contatti inibisce l'esecuzione del comando di arresto. Anche in questo caso, la protezione chiusa impedisce l'accesso al pericolo.

I componenti di sicurezza del sistema di controllo si devono interfacciare con i componenti non legati alla sicurezza. Poiché i guasti dei dispositivi di controllo di avviamento e arresto non dovrebbero provocare la perdita della funzione di sicurezza, questi dispositivi non sono considerati parte integrante del sistema di sicurezza. Questo circuito di Avviamento/Arresto/Mantenimento rappresenta i componenti senza caratteristiche di sicurezza della circuiteria di controllo della macchina che possono essere sostituiti con un PLC.

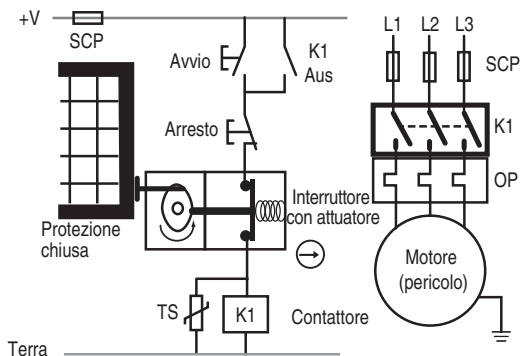
La Categoria B rappresenta la base della progettazione di un sistema di sicurezza. Anche se la correttezza delle fasi di progettazione, selezione e installazione è la premessa di un sistema robusto, diversi singoli fattori possono comportare la perdita del sistema di sicurezza. Tenendo conto di questi fattori, le possibilità di guasti in grado di generare pericoli possono essere ulteriormente minimizzate. L'uso esclusivo della Categoria B non è adatto alla maggior parte delle applicazioni di sicurezza.

Categoria 1

La Categoria 1 richiede che il sistema sia conforme ai termini della Categoria B e che usi componenti di sicurezza di comprovata efficienza. Che cosa sono esattamente i componenti di sicurezza e come sappiamo se sono di comprovata efficienza? ISO 13849-2 ci aiuta a rispondere a queste domande per i sistemi elettrici, pneumatici, idraulici e meccanici. L'Allegato D tratta i componenti elettrici.

I componenti sono considerati di comprovata efficienza se sono stati usati con successo in molte altre simili applicazioni. I componenti di sicurezza progettati recentemente sono considerati di comprovata efficienza se concepiti e verificati in conformità ai corrispondenti standard.

Componente di comprovata efficienza	Standard
Interruttore a modalità di apertura positiva (apertura diretta)	IEC 60947-5-1
Dispositivo di arresto di emergenza	ISO 13850, IEC 60947-5-5
Fusibile	IEC 60269-1
Interruttore automatico	IEC 60947-2
Contattori	IEC 60947-4-1, IEC 60947-5-1
Contatti ad accoppiamento meccanico	IEC 60947-5-1
Contattore ausiliario (ad es. contattore, relè ausiliario, relè a guida forzata)	EN 50205 IEC 60204-1, IEC 60947-5-1
Trasformatore	IEC 60742
Cavo	IEC 60204-1
Dispositivi di interblocco	ISO 14119
Termostato	IEC 60947-5-1
Pressostato	IEC 60947-5-1 + requisiti pneumatici o idraulici
Apparecchiatura o dispositivo di commutazione di protezione e controllo (CPS)	IEC 60947-6-2
Controllore a logica programmabile	IEC 61508, IEC 62061

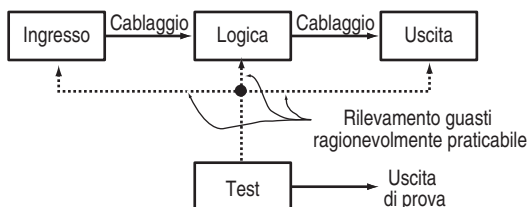
Applicando componenti di comprovata efficienza al nostro sistema di Categoria B, l'interruttore di finecorsa sarebbe sostituito da un interruttore con attuatore ad azione di apertura diretta e il contattore sarebbe sovradimensionato per una maggiore protezione contro la saldatura dei contatti.

Semplice sistema di sicurezza di Categoria 1

Qui sono riportate le modifiche a un semplice sistema di Categoria B, per ottenere la Categoria 1. Interblocco e contattore svolgono il ruolo chiave di scollegare l'alimentazione all'attuatore, quando è necessario accedere al pericolo. L'interblocco con attuatore risponde ai requisiti IEC 60947-5-1 per i contatti ad azione di apertura diretta (contrassegnato, nel disegno, dalla freccia nel cerchio). Con componenti di comprovata efficienza, la probabilità che l'alimentazione venga scollegata è più alta per la Categoria 1 che per la Categoria B. L'uso di componenti di comprovata efficienza serve a impedire la perdita della funzione di sicurezza. Anche con questi miglioramenti, un singolo guasto può comunque comportare la perdita della funzione di sicurezza.

Possiamo applicare questi stessi principi al sistema di categoria B basato su PLC per portare le prestazioni di sicurezza alla Categoria 1? Si può procedere in entrambi i sensi. Sicuramente, sostituendo tutti gli interruttori di finecorsa che funzionano in modalità negativa con interblocchi ad azione di apertura diretta e sovradimensionando i contattori, si aumenta la probabilità di realizzare la funzione di sicurezza. In tal caso, è necessario concentrare l'attenzione sul PLC. Il PLC è stato usato in altre simili applicazioni? Il programma logico è convalidato e stabile o ancora in evoluzione? Il firmware (quella parte del software che l'utente non può modificare) è stato revisionato di recente? In applicazioni simili, qual è la storia dei guasti hardware in grado di generare situazioni di pericolo? Sono state adottate misure per eliminare o ridurre questi guasti a livelli accettabili? In teoria, è possibile che un PLC possa essere considerato un componente di comprovata efficienza in quanto soluzione progettuale consolidata. Per adottare questo approccio per un dispositivo come un PLC, sarebbe estremamente impegnativo considerare un livello troppo alto di acquisizione e analisi dei dati. Per semplificare la situazione ed evitare l'uso arbitrario di PLC "ordinari", ISO 13849-1:1999 stabilisce che "a livello di singoli componenti elettronici, non è di solito possibile ottenere la Categoria 1".

Le Categorie B e 1 sono basate sulla prevenzione. La concezione è intesa a prevenire le situazioni pericolose. Quando la sola prevenzione non consente una sufficiente riduzione del rischio, bisogna ricorrere al rilevamento dei guasti. Le Categorie 2, 3 e 4 sono basate sul rilevamento dei guasti, con requisiti sempre più rigidi per ottenere sempre maggiori livelli di riduzione dei rischi.

Categoria 2

Oltre a rispondere ai requisiti della Categoria B e a utilizzare principi di sicurezza di comprovata efficienza, il sistema di sicurezza deve essere sottoposto a test per rispondere ai requisiti della Categoria 2. I test devono essere concepiti per rilevare guasti nei componenti di sicurezza del sistema di controllo. Se non viene rilevato alcun guasto, la macchina può entrare in funzione. In presenza di guasti, il test deve generare un comando. Quando possibile, il comando deve portare la macchina in stato di sicurezza.

Il test deve permette di rilevare i guasti in modo ragionevolmente praticabile. L'apparecchiatura che effettua il test può essere parte integrante del sistema di sicurezza o uno strumento separato.

Il test deve essere realizzato nelle seguenti condizioni:

- alla prima accensione della macchina,
- prima della generazione di un pericolo, e
- periodicamente, se ritenuto necessario dalla valutazione dei rischi

Le parole "quando possibile" e "ragionevolmente praticabile" indicano che non tutti i guasti sono rilevabili. Trattandosi di un sistema a canale singolo (ovvero un unico cavo collega, in sequenza, ingresso-logica-uscita), un singolo guasto può comportare la perdita della funzione di sicurezza. In alcuni casi, la Categoria 2 non può essere completamente applicata a un sistema di sicurezza, perché non tutti i componenti possono essere controllati.

Sistema di sicurezza di Categoria 2

Questo è un semplice sistema di Categoria 1, migliorato per rispondere alla Categoria 2. Un relè di monitoraggio di sicurezza (MSR) realizza il test. All'accensione, l'MSR controlla i suoi componenti interni. Se non viene rilevato alcun guasto, l'MSR controlla l'interruttore con attuatore monitorando la funzionalità dei suoi contatti. Se non viene rilevato alcun guasto e la protezione è chiusa, l'MSR controlla il dispositivo di uscita: i contatti ad accoppiamento meccanico del contattore. Se non viene rilevato alcun guasto e il contattore è disattivato, l'MSR eccita la sua uscita interna e collega la bobina di K1 al pulsante di arresto. A questo punto, i componenti non legati alla sicurezza del sistema di controllo della macchina, il circuito di Avviamento/Arresto/Interblocco, possono accendere e spegnere la macchina.

Aprendo la protezione, si disattivano le uscite dell'MSR. Quando la protezione viene richiusa, l'MSR ripete i controlli sul sistema di sicurezza. Se non viene rilevato alcun guasto, l'MSR attiva la sua uscita interna. L'MSR permette a questo circuito di rispondere alla Categoria 2 testando il dispositivo di ingresso, il dispositivo logico (se stesso) e il dispositivo di uscita. Il test è eseguito alla prima accensione e prima dell'inizio del pericolo.

Con le sue capacità logiche intrinseche, un sistema di sicurezza basato su PLC può essere concepito per rispondere alla Categoria 2. Come stabilito nella precedente trattazione della Categoria 1, il punto diventa la giustificazione di comprovata efficienza del PLC (tra cui le sue capacità di test). Per sistemi di sicurezza complessi che richiedono una classificazione di Categoria 2, un PLC non di sicurezza dovrebbe essere sostituito con un PLC di sicurezza conforme a IEC 61508.

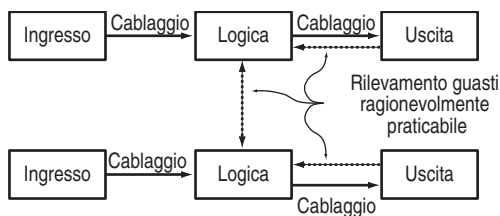
Sistema di sicurezza complesso di Categoria 2

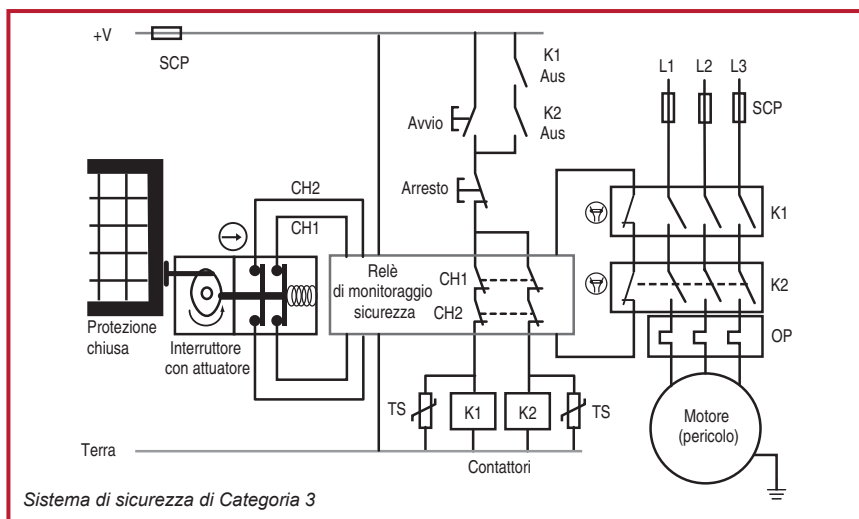
Questo è l'esempio di un sistema complesso che usa un PLC di sicurezza. Un PLC di sicurezza, essendo concepito secondo un determinato standard, risponde ai requisiti di comprovata efficienza. I contatti ad accoppiamento meccanico dei contattori sono portati all'ingresso del PLC a scopo di test. A seconda della logica di programma, questi contatti possono essere collegati in serie a un terminale di ingresso o a singoli terminali di ingresso.

Anche se vengono utilizzati componenti di sicurezza di comprovata efficienza, un singolo guasto tra i controlli può comportare la perdita della funzione di sicurezza. Quindi, i sistemi di Categoria 2 sono utilizzati nelle applicazioni a rischio più basso. Quando sono necessari livelli più alti di tolleranza ai guasti, il sistema di sicurezza deve essere di Categoria 3 o 4.

Categoria 3

Oltre a rispondere ai requisiti della Categoria B e ai principi di sicurezza di comprovata efficienza, la Categoria 3 richiede l'operatività della funzione di sicurezza in presenza di un singolo guasto. Il guasto deve essere rilevato in concomitanza o prima della successiva richiesta di intervento della funzione di sicurezza, ogniqualvolta ragionevolmente praticabile.

Di nuovo, abbiamo la frase "ogniqualvolta ragionevolmente praticabile". Ciò considera i guasti che possono non essere rilevati. Fino a che il guasto non rilevabile non comporta la perdita della funzione di sicurezza, la funzione di sicurezza può rispondere alla Categoria 3. Di conseguenza, un accumulo di guasti non rilevabili può comportare la perdita della funzione di sicurezza.

Lo schema a blocchi qui presentato spiega i principi di un sistema di Categoria 3. Per monitorare le prestazioni della funzione di sicurezza, si ricorre alla ridondanza e al monitoraggio incrociato e delle uscite, quando ragionevolmente praticabile.

Sistema di sicurezza di Categoria 3

Questo è un esempio di sistema di Categoria 3. Un set ridondante di contatti viene aggiunto all'interruttore di interblocco con attuatore. Internamente, il relè di monitoraggio di sicurezza (MSR) contiene circuiti ridondanti che si monitorano reciprocamente. Un set ridondante di contattori toglie alimentazione al motore. I contattori sono monitorati dall'MSR attraverso i contatti ad accoppiamento meccanico nel modo "ragionevolmente praticabile".

Il rilevamento dei guasti deve considerare ogni componente del sistema di sicurezza, oltre che i collegamenti (ovvero il sistema). Quali sono le modalità di guasto di un interruttore con attuatore a due canali? Quali sono le modalità di guasto dell'MSR? Quali sono le modalità di guasto dei contattori K1 e K2? Quali sono le modalità di guasto del cablaggio?

L'interruttore interbloccato con attuatore è concepito con contatti ad apertura diretta. Quindi sappiamo che l'apertura della protezione è concepita per aprire un contatto saldato. Questo risolve una modalità di guasto. Esistono altre modalità di guasto?

L'interruttore ad azione di apertura diretta è di solito concepito con un ritorno a molla. Se la testa viene rimossa o staccata, i contatti di sicurezza tornano in stato di chiusura (sicuro). Molti interruttori di interblocco sono concepiti con teste rimovibili, per adattarsi ai requisiti di installazione di varie applicazioni. La testa può essere rimossa e ruotata tra due e quattro posizioni.

Se le viti di montaggio della testa non sono correttamente serrate, potrebbe verificarsi un guasto. In questa condizione, le vibrazioni della macchina possono provocare l'uscita delle viti di montaggio della testa. La testa, sotto la pressione della molla, rilascia i contatti di sicurezza che, quindi, si chiudono. Di conseguenza, l'apertura della protezione non apre i contatti di sicurezza e si verifica un guasto in grado di generare un pericolo.

In modo simile, anche il meccanismo operativo all'interno dell'interruttore deve essere esaminato. Qual è la probabilità che il guasto di un singolo componente comporti la perdita della funzione di sicurezza? Le risposte a queste domande si avranno più avanti dato che, per assicurare l'operatività della funzione di sicurezza, occorre considerare il ruolo del tempo medio prima di un guasto pericoloso, della copertura diagnostica e della percentuale di guasti sicuri.

Una pratica comune è l'uso di interblocchi con attuatore con doppi contatti in circuiti di Categoria 3. Ciò deve essere basato sull'esclusione del singolo guasto dell'interruttore per aprire i contatti di sicurezza. Si tratta della cosiddetta "esclusione del guasti", trattata più avanti in questo capitolo.

Un relè di monitoraggio di sicurezza elettromeccanico (MSR) è un dispositivo a bassa complessità, spesso valutato da terzi, a cui viene assegnata una categoria. L'MSR prevede spesso capacità a doppio canale, monitoraggio incrociato dei canali e dei dispositivi esterni, protezione dai cortocircuiti. Non esiste alcuno specifico standard sulla concezione o l'uso dei relè di monitoraggio di sicurezza. Gli MSR sono valutati, in base alla loro capacità di realizzare la funzione di sicurezza, secondo ISO 13849-1 o il precedente EN 954-1. Per adeguarsi alla categoria di un sistema di sicurezza, l'MSR deve avere una classificazione uguale o più alta.

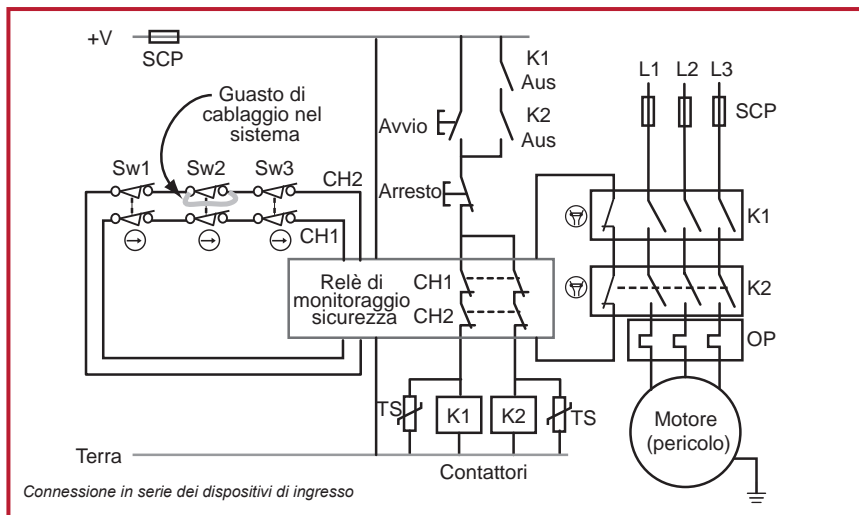
Due contattori aiutano a garantire che i dispositivi di uscita realizzino la funzione di sicurezza. Con una protezione contro i sovraccarichi e i cortocircuiti, la probabilità che il contattore abbia problemi di contatti saldati è scarsa, ma non impossibile. Un contattore può generare un guasto anche a causa di contatti di commutazione chiusi per incollatura dell'indotto. Se il guasto di un contattore genera uno stato pericoloso, il secondo contattore toglie alimentazione alla fonte del pericolo. L'MSR rileva il contattore in guasto al successivo ciclo della macchina. Quando la protezione è chiusa e il pulsante di avviamento premuto, i contatti ad accoppiamento meccanico del contattore in guasto rimangono aperti e l'MSR, non essendo in grado di chiudere i contatti di sicurezza, rivela il guasto.

Guasti non rilevati

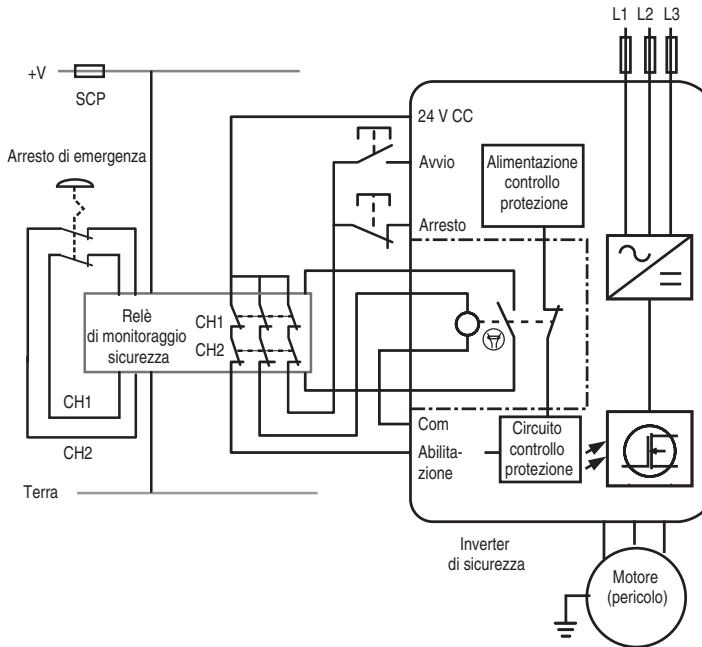
Come spiegato precedentemente, alcuni guasti non possono essere rilevati. Questi guasti, da soli, non comportano la perdita della funzione di sicurezza. Quando si valutano i guasti, occorre farsi una serie di domande. La risposta alla prima domanda deciderà le domande successive: *Domanda di apertura:* Il guasto può essere rilevato?

Se sì, dobbiamo sapere se questo rilevamento è immediato o in occasione della successiva richiesta. Abbiamo anche bisogno di sapere se può essere mascherato (ovvero cancellato) da altri dispositivi.

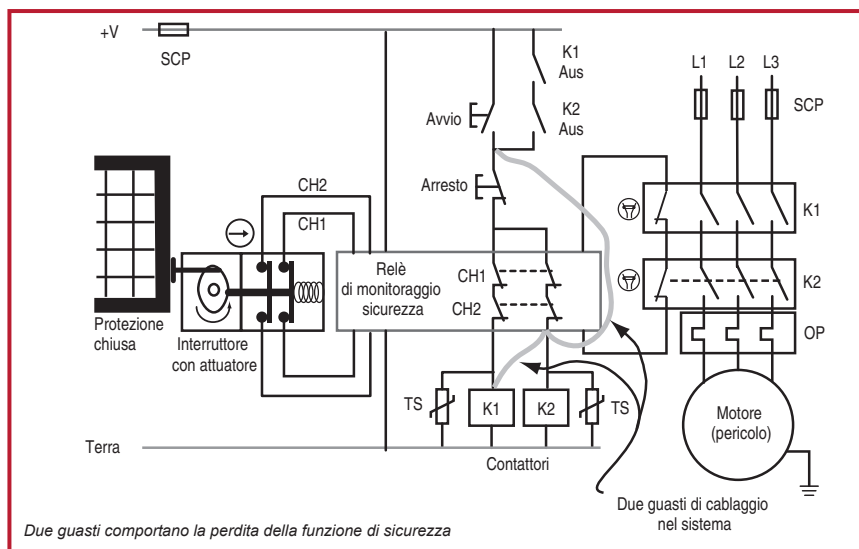
Se no, il guasto può comportare la perdita della funzione di sicurezza? Un guasto conseguente può comportare la perdita della funzione di sicurezza?

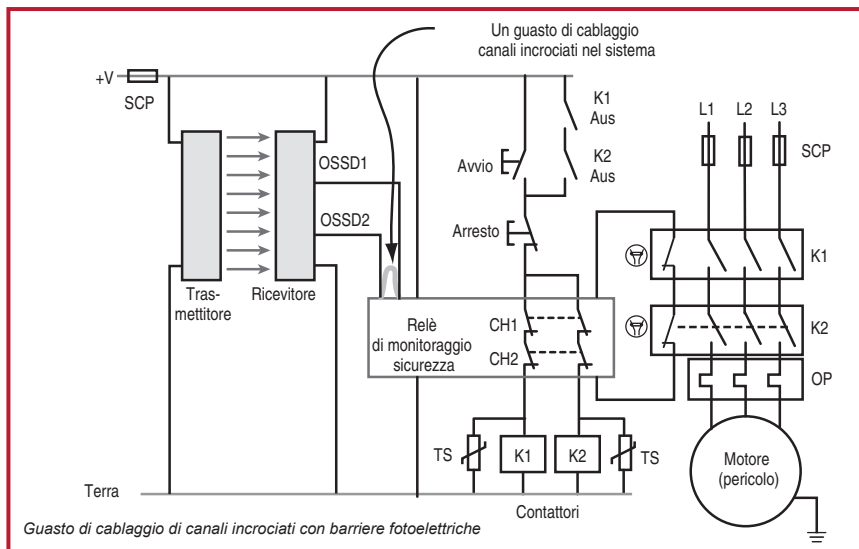
Connessione in serie dei dispositivi di ingresso

L'approccio qui riportato è ampiamente utilizzato per collegare molteplici dispositivi a un relè di monitoraggio di sicurezza. Ogni dispositivo contiene due contatti ad azione di apertura diretta, normalmente chiusi. Questi dispositivi possono essere una combinazione di interblocchi o pulsanti di arresto di emergenza. Dato che i dispositivi di ingresso sono collegati a margherita, questo approccio consente di risparmiare sui costi di cablaggio. Presumiamo che, attraverso uno dei contatti, si verifichi un cortocircuito. Il guasto può essere rilevato?

Quando gli interruttori Sw1 e Sw3 sono aperti, l'MSR scollega l'alimentazione al pericolo. Quando Sw1 e Sw3 sono chiusi, il pericolo può essere riavviato premendo il pulsante di avviamento. Durante queste azioni, il guasto non è stato rilevato ma non ha comportato la perdita della funzione di sicurezza. Che succede quando Sw2 è aperto?

Quando Sw2 si apre, Ch1 si apre e Ch2 rimane chiuso. L'MSR diseccita il pericolo perché Ch1 è aperto. Quando Sw2 si chiude, il motore non può essere avviato con il pulsante di avviamento premuto, perché Ch2 non si è aperto. Il guasto viene rilevato. Il punto debole di questo concetto è che l'interruttore Sw1 o Sw3 può essere aperto o chiuso e mascherare il guasto. Un guasto successivo (un cortocircuito attraverso il secondo contatto o Sw2) comporterà la perdita della funzione di sicurezza. Il collegamento in serie dei contatti meccanici è limitato alla Categoria 3, dato che può portare alla perdita della funzione di sicurezza a causa dell'accumulo di guasti.

Questo è un circuito di Categoria 3 che usa inverter di sicurezza a frequenza variabile. I recenti sviluppi delle tecnologie di azionamento, in combinazione con l'aggiornamento degli standard elettrici, permettono di usare gli inverter di sicurezza nei circuiti di arresto di emergenza, senza bisogno di un sezionatore elettromeccanico dell'attuatore (ad es. il motore).

Premendo il pulsante di emergenza si aprono le uscite dell'MSR. Questo invia un segnale di arresto all'inverter, rimuove il segnale di abilitazione e interrompe l'alimentazione del controllo di gate. L'inverter esegue un arresto di Categoria 0 – immediato scollegamento dell'alimentazione al motore. L'inverter raggiunge la Categoria 3 perché ha segnali ridondanti per togliere alimentazione al motore: il segnale di abilitazione e un relè a guida forzata. Il relè a guida forzata fornisce all'attuatore il feedback ragionevolmente praticabile. Lo stesso inverter viene analizzato per determinare che un singolo guasto non comporti la perdita della funzione di sicurezza.

Due guasti comportano la perdita della funzione di sicurezza

Questo è un secondo guasto che comporta la perdita della funzione di sicurezza. Si tratta di un corto tra l'uscita dell'MSR e il pulsante di avviamento. All'accensione con protezione chiusa, questi due guasti non vengono rilevati. Premendo il pulsante di avviamento, inizia il pericolo. L'apertura della protezione non provoca la disattivazione del pericolo.

Guasto di cablaggio di canali incrociati con barriere fotoelettriche

Questo è un esempio di sistema di sicurezza con barriera fotoelettrica (uscite OSSD)

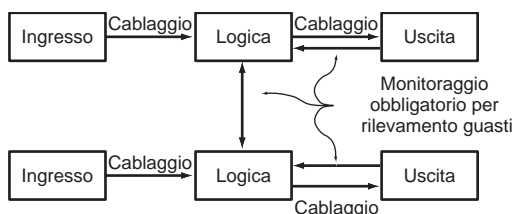
Il sistema di sicurezza può rilevare questo guasto?

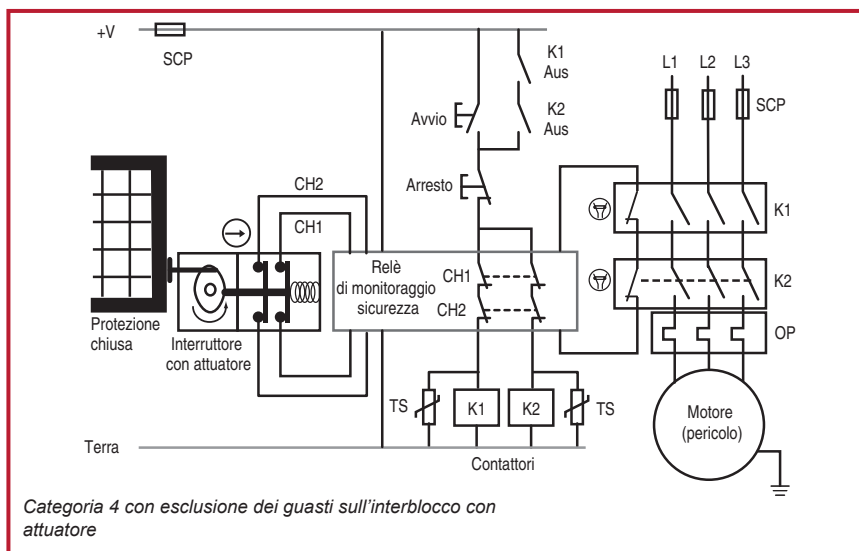
L'MSR non può rilevare questo guasto, perché entrambi gli ingressi sono in "pull up" a +V. In questo esempio, il guasto di cablaggio è rilevato dalla barriera fotoelettrica. Alcune barriere fotoelettriche usano una tecnica di rilevamento dei guasti chiamata "test a impulsi". Con queste barriere fotoelettriche, il rilevamento del guasto è immediato e la barriera fotoelettrica disattiva la sua uscita. In altre, il rilevamento avviene quando la barriera fotoelettrica è liberata. Quando la barriera fotoelettrica tenta di eccitare la sua uscita, il guasto viene rilevato e l'uscita rimane disattivata. In entrambi i casi, il pericolo rimane disattivato in presenza del guasto.

Rilevamento dei guasti mediante test a impulsi

I circuiti di sicurezza sono concepiti per condurre corrente quando il sistema di sicurezza è attivo e il pericolo è protetto. Il test a impulsi è una tecnica per cui la corrente del circuito scende a zero per un periodo molto breve. La durata è troppo breve perché il circuito di sicurezza risponda e disattivi il pericolo, ma è abbastanza lunga per il rilevamento da parte di un sistema a microprocessore. Gli impulsi sui canali sono sfasati uno rispetto all'altro. Se si verifica un cortocircuito incrociato, il microprocessore rileva gli impulsi su entrambi i canali e genera un comando di disattivazione del pericolo.

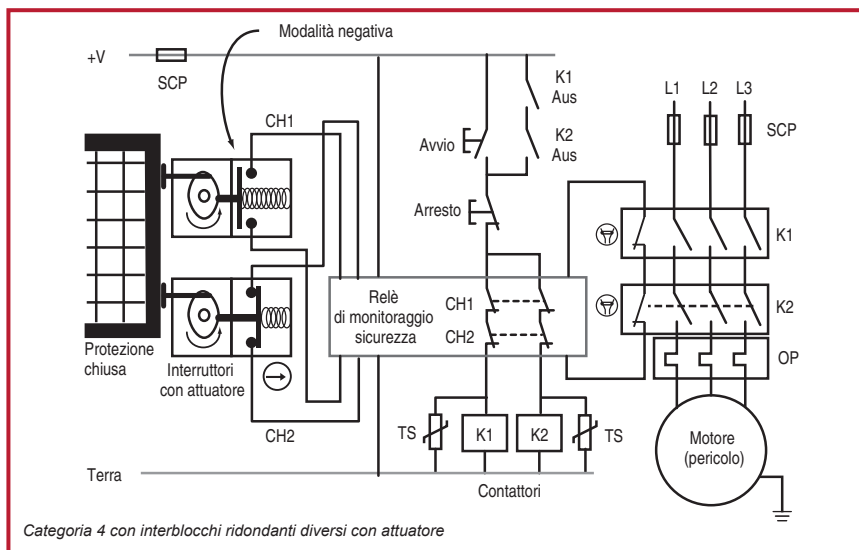
Categoria 4

Come la Categoria 3, la Categoria 4 impone che il sistema di sicurezza risponda alla Categoria B, usi principi di sicurezza e realizzi la funzione di sicurezza in presenza di un singolo guasto. Diversamente dalla Categoria 3, dove un accumulo di guasti può portare alla perdita della funzione di sicurezza, la Categoria 4 richiede l'operatività della funzione di sicurezza in presenza di un accumulo di guasti. Quando si considera un accumulo di guasti, 2 guasti possono essere sufficienti anche se, per alcune configurazioni, possono essere necessari 3 guasti.

Questo è lo schema a blocchi per la Categoria 4. Il monitoraggio di entrambi i dispositivi di uscita e il monitoraggio incrociato sono requisiti essenziali, non solo quando ragionevolmente praticabile. Questo contribuisce a differenziare la Categoria 4 dalla Categoria 3.

Categoria 4 con esclusione dei guasti sull'interblocco con attuatore

Questo è un esempio di circuito di Categoria 4 con esclusione dei guasti sull'interblocco con attuatore. L'esclusione dei guasti elimina la considerazione del guasto di apertura dei contatti dell'interblocco con attuatore. L'esclusione del guasto deve essere tecnicamente giustificata e documentata. Nella giustificazione, devono essere considerati velocità e allineamento dell'attuatore, arresti meccanici e protezione della testa.

Se il progettista del sistema di sicurezza preferisce usare interblocchi con attuatore ma non si trova con l'uso dell'esclusione dei guasti sugli interblocchi, per rispondere alla Categoria 4 possono essere usati due interblocchi con attuatore. Lo stesso relè di monitoraggio di sicurezza deve essere classificato adatto alla Categoria 4 ed entrambi i contattori di uscita con contatti ad accoppiamento meccanico devono essere monitorati.

La diversità può essere applicata per ridurre ulteriormente la probabilità di perdita della funzione di sicurezza dovuta a guasti per causa comune; uno degli interruttori interbloccati con attuatore può essere convertito in modalità negativa. Un interruttore che funziona in modalità negativa è accettabile se un secondo interruttore usa contatti ad azione di apertura diretta. Lo schema che segue mostra un esempio di questo approccio di diversità. Con questo approccio, l'MSR deve essere concepito per accettare ingressi normalmente aperti e normalmente chiusi.

Categoria 4 con interblocchi ridondanti diversi con attuatore

Classificazione di sistemi e componenti

ISO 13849-1 richiede la classificazione sia dei componenti sia dei sistemi. Questo genera un po' di confusione che può essere superata conoscendo i componenti e le loro capacità. Si evince che, a seconda dell'architettura del sistema, un componente di Categoria 1 può essere usato in un sistema di Categoria 2, 3 o 4.

Le categorie B e 1 sono basate sulla prevenzione, mentre le categorie 2, 3 e 4 sono basate sul rilevamento. Queste categorie valgono sia per i componenti che per i sistemi. Il sistema di sicurezza standard consiste in un interruttore di interblocco di sicurezza, un relè di sicurezza e un contattore di sicurezza. L'interblocco e il contattore sono classificati come dispositivi di

Categoria 1, perché basati solo sulla prevenzione. Utilizzano principi di sicurezza ma non effettuano alcun rilevamento o autodiagnostica. Questi dispositivi possono essere usati in ridondanza nei sistemi di Categoria 3 e 4, ammesso che il dispositivo logico effettui il rilevamento.

I dispositivi logici non sono basati solo sulla prevenzione ma anche sul rilevamento. Internamente, si controllano da soli per assicurare la corretta funzionalità. Quindi, relè di monitoraggio e controllori programmabili di sicurezza sono classificati per le Categorie 2, 3 o 4.

Considerazione ed esclusione dei guasti

L'analisi della sicurezza richiede una ampia analisi dei guasti e una perfetta comprensione della funzionalità del sistema di sicurezza in presenza di guasti. ISO 13849-1 e ISO 13849-2 forniscono dettagli sulla considerazione e l'esclusione dei guasti.

Se un guasto comporta il guasto di un componente successivo, esso deve essere considerato, insieme a tutti quelli successivi, come un unico guasto.

Se due o più guasti avvengono come risultato di una singola causa, devono essere considerati come un unico guasto. Questo è ciò che si definisce "guasto per causa comune".

Il verificarsi simultaneo di due o più guasti è considerato altamente improbabile e non è affrontato in questa analisi. Tra le richieste di intervento a un sistema di sicurezza, l'ipotesi di base è che si verifichi un solo guasto.

Quando componenti e sistemi sono concepiti secondo i corrispondenti standard, il verificarsi del guasto può essere escluso. Ad esempio, l'apertura di contatti normalmente chiusi può essere esclusa se l'interruttore è costruito secondo IEC 60947-5-1 Allegato K. ISO 13849-2 fornisce una lista delle esclusioni di guasto.

Sistemi con arresti di Categoria 1

Tutti gli esempi sopra riportati hanno mostrato arresti di Categoria 0 (immediato scollegamento dell'alimentazione agli attuatori). Un arresto di Categoria 1 (frenatura fino al raggiungimento dell'arresto e, successivamente, scollegamento dell'alimentazione all'attuatore) si ottiene con un'uscita temporizzata. Un arresto di Categoria 1 è spesso associato a una protezione interbloccata con blocco della protezione. Questo fa sì che la protezione rimanga bloccata in posizione di chiusura fino a quando la macchina raggiunge uno stato di sicurezza (arresto).

Arrestare una macchina senza tener conto del controllore programmabile può influire sul riavviamento e potrebbe essere causa di gravi danni agli utensili e alla macchina. Per l'arresto di sicurezza, non ci si può affidare a un PLC standard (non di sicurezza) e, quindi, devono essere considerati altri approcci.

Di seguito, sono riportate tre possibili soluzioni:

1. PLC di sicurezza

Uso di un PLC con un livello di integrità della sicurezza sufficientemente alto per essere usato in sistemi di sicurezza. In pratica, questo si otterrebbe con un PLC di sicurezza come GuardLogix sia per il controllo di sicurezza sia per quello standard.

2. Relè di sicurezza con comando di override temporizzato

Viene utilizzato un relè di sicurezza con uscite immediate e temporizzate (ad es. MSR138DP). Le uscite ad azione immediata sono collegate a ingressi del dispositivo programmabile (ad esempio un P.L.C.) e le uscite temporizzate sono collegate al contattore. Quando l'interruttore di interblocco della protezione è attivato, le uscite immediate del relè di sicurezza commutano. Questo segnala al sistema programmabile di eseguire un arresto secondo la sequenza corretta. Dopo un periodo di tempo sufficiente per l'esecuzione del processo, l'uscita temporizzata del relè di sicurezza scatta e isola il contattore principale.

Nota: tutti i calcoli che servono a determinare il periodo di arresto totale devono prendere in considerazione il ritardo di uscita del relè di sicurezza. Questo è particolarmente importante quando questo fattore viene usato per determinare il posizionamento dei dispositivi in conformità con il calcolo della distanza di sicurezza.

3. Dispositivi di blocco della protezione controllati dal sistema programmabile

Questa soluzione offre un elevato livello di integrità garantito dal cablaggio unito alla capacità di fornire un arresto che segue una sequenza corretta ma può essere applicato solo nel caso in cui il pericolo sia protetto da una protezione.

Per consentire l'apertura della porta di protezione, l'elettroserratura dell'interruttore di interblocco deve ricevere un segnale di rilascio dal PLC. Questo segnale viene inviato solo al termine della sequenza di arresto, per ridurre il rischio di danni agli utensili o perdita del

programma. Quando il solenoide viene eccitato, la porta può essere aperta e i contatti del circuito di controllo sull'interruttore di interblocco isolano il contattore della macchina. Per poter superare eventuali arresti rallentati della macchina o segnali di rilascio spuri, potrebbe essere necessario usare un'unità temporizzata (ad es. MSR178DP) o un rilevatore di movimento arrestato (ad es. CU2) insieme al PLC.

Requisiti dei sistemi di controllo di sicurezza USA

Negli USA, esiste tutta una serie di diversi standard sui requisiti dei sistemi di controllo legati alla sicurezza ma due sono i documenti più importanti: ANSI B11.TR3 e ANSI R15.06. Il rapporto tecnico ANSI B11.TR3 stabilisce quattro livelli caratterizzati dal livello previsto di riduzione dei rischi che ognuno può fornire.

Ecco i requisiti per ogni livello.

Livello minimo di riduzione dei rischi

In ANSI B11.TR3, tra le protezioni che forniscono il minimo grado di riduzione dei rischi ci sono dispositivi elettrici, elettronici, idraulici o pneumatici e relativi sistemi di controllo con configurazione a canale singolo. Implicita nei requisiti è l'esigenza di usare dispositivi di sicurezza. Questo livello è strettamente allineato con la Categoria 1 di ISO 13849-1.

Livello medio/basso di riduzione dei rischi

In ANSI B11.TR3, le protezioni di sicurezza che offrono una riduzione dei rischi medio/bassa includono i sistemi di controllo ridondanti che possono essere controllati manualmente per verificare la funzionalità del sistema di sicurezza. Facendo esclusivamente riferimento ai requisiti, il sistema prevede una ridondanza semplice. L'uso di una funzione di controllo non è richiesta. Senza controllo, l'eventuale guasto di uno dei componenti di sicurezza ridondanti potrebbe non essere rilevato dal sistema di sicurezza. Ciò risulterebbe in un sistema a singolo canale. Questo livello di riduzione dei rischi si allinea meglio con la Categoria 2 in associazione al controllo.

Livello medio/alto di riduzione dei rischi

Le protezioni di sicurezza che, per ANSI B11.TR3, forniscono una riduzione dei rischi medio/alta includono sistemi di controllo con ridondanza e autodiagnostica all'avviamento, per confermare la funzionalità del sistema di sicurezza. Per le macchine che vengono avviate ogni giorno, l'autodiagnostica rappresenta un significativo miglioramento dell'integrità della sicurezza rispetto a un sistema puramente ridondante. Per le macchine che funzionano 24 ore al giorno, 7 giorni su 7, l'autodiagnostica è un miglioramento marginale. Con il monitoraggio periodico del sistema di sicurezza, si allinea con la Categoria 3.

Livello massimo di riduzione dei rischi

ANSI B11.TR3 identifica la più alta riduzione dei rischi con sistemi di controllo ridondanti e con autodiagnostica continua. L'autodiagnostica deve verificare la funzionalità del sistema di sicurezza. L'obiettivo, per il progettista del sistema di sicurezza, è determinare che cosa si intende per "autodiagnostica continua". Molti sistemi di sicurezza effettuano i loro controlli all'avviamento e in presenza di una richiesta di intervento al sistema di sicurezza.

Alcuni componenti, d'altra parte, effettuano una autodiagnostica continua. Le barriere fotoelettriche, per esempio, accendono e spengono sequenzialmente i loro LED. Se si verifica un guasto, la barriera fotoelettrica disattiva le sue uscite, prima della richiesta di intervento al sistema di sicurezza, dato che esso si controlla continuamente. I PLC di sicurezza e i relè a microprocessore sono altri componenti che effettuano autodiagnostica continua.

Il requisito del sistema di controllo riguardante l'autodiagnostica "continua" non vuole limitare la selezione dei componenti a barriere fotoelettriche e unità logiche a microprocessore. Il controllo dovrebbe essere realizzato all'avviamento e dopo ogni richiesta di intervento al sistema di sicurezza. Questo livello di riduzione dei rischi si allinea con la Categoria 4 di ISO 13849-1.

Standard per i robot: Stati Uniti/Canada

Gli standard per i robot negli USA (ANSI RIA R15.06) e in Canada (CSA Z434-03) sono simili. Entrambi hanno quattro livelli, simili alle categorie di EN 954-1:1996.

Semplice

Al livello più basso, semplici sistemi di controllo di sicurezza devono essere progettati e costruiti con circuiteria approvata a canale singolo e questi sistemi possono essere programmabili. In Canada, questo livello è ulteriormente limitato esclusivamente ad attività di segnalazione e annuncio. Per il progettista del sistema di sicurezza, il punto è determinare che cosa è "approvato". Che cos'è un circuito a singolo canale approvato? E da chi il sistema è approvato? La categoria Semplice è strettamente allineata con la Categoria B di EN 954-1:1996.

Canale singolo

Il livello successivo è il sistema di controllo di sicurezza a canale singolo che

- è basato su hardware o è un dispositivo software/firmware di sicurezza
- integra componenti di sicurezza; e
- è utilizzato secondo le raccomandazioni dei costruttori e
- usa configurazioni di circuito comprovate.

Un esempio di “configurazione di circuito comprovata” è un dispositivo elettromeccanico, ad apertura positiva e a singolo canale, che segnala un arresto in stato di diseccitazione. Trattandosi di un sistema a canale singolo, il guasto di un singolo componente può comportare la perdita della funzione di sicurezza. Questa categoria è strettamente allineata con la Categoria 1 di EN 954-1:1996.

Dispositivi software/firmware di sicurezza

Sebbene i sistemi hardware siano stati il metodo preferito per la protezione di sicurezza dei robot, i dispositivi software/firmware si stanno affermando sempre maggiormente grazie alla loro capacità di gestire sistemi complessi. I dispositivi software/firmware (PLC o controllori di sicurezza) sono ammessi purché siano di sicurezza. Questa classificazione impone che un singolo guasto del firmware o di un componente di sicurezza non comporti la perdita della funzione di sicurezza. Quando il guasto viene rilevato, il successivo funzionamento automatico del robot viene impedito fino alla cancellazione del guasto.

Per ottenere una classificazione di sicurezza, il dispositivo software/firmware deve essere testato, in base a uno standard approvato, da un laboratorio certificato Negli USA, l’OSHA mantiene aggiornata una lista dei laboratori di prova riconosciuti a livello nazionale (NRTL). In Canada, lo Standard Council of Canada (SCC) dispone di una lista simile.

Singolo canale con monitoraggio

I sistemi di controllo di sicurezza a singolo canale con monitoraggio devono rispettare tutti i requisiti richiesti per il singolo canale, essere di sicurezza e avere funzionalità di controllo. Il controllo delle funzioni di sicurezza deve essere effettuato all’avviamento della macchina e, periodicamente, durante il funzionamento. Il controllo automatico è preferibile a quello manuale.

L’operazione di controllo permette il funzionamento se non viene rilevato alcun guasto o genera un segnale di arresto se il guasto viene rilevato. Eventuali pericoli persistenti dopo la cessazione del movimento devono essere segnalati. Naturalmente, il controllo stesso non deve provocare una situazione pericolosa. Dopo il rilevamento del guasto, il robot deve rimanere in stato di sicurezza fino alla correzione del guasto.

Questa categoria è in linea con la Categoria 2 di EN 954-1:1996.

Controllo affidabile

Il più alto livello di riduzione dei rischi negli standard per i robot, in USA e Canada, si ottiene attraverso i sistemi di controllo di sicurezza di tipo a controllo affidabile. I sistemi di controllo di sicurezza a controllo affidabile sono architetture a due canali con monitoraggio. La funzione di arresto del robot non deve essere impedita dal guasto di alcun singolo componente, neanche dalla funzione di monitoraggio.

Al rilevamento di un guasto, il monitoraggio deve generare un comando di arresto. Eventuali pericoli persistenti dopo la cessazione del movimento devono essere segnalati. Il sistema di sicurezza deve rimanere in stato di sicurezza fino alla correzione del guasto.

Preferibilmente, il guasto deve essere rilevato immediatamente. Se ciò non è possibile, deve essere rilevato alla successiva richiesta di intervento al sistema di sicurezza.

Se c'è una significativa probabilità che possano verificarsi, i guasti per causa comune devono essere considerati.

I requisiti canadesi differiscono dai requisiti USA per l'aggiunta di due ulteriori requisiti. Primo, i sistemi di controllo di sicurezza devono essere indipendenti dai normali sistemi di controllo di programma. Secondo, il sistema di sicurezza non deve essere facilmente escluso o bypassato senza rilevamento.

I sistemi a controllo affidabile sono in linea con le Categoria 3 e 4 di EN 954-1:1996.

Note sui sistemi a controllo affidabile

L'aspetto fondamentale dei sistemi a controllo affidabile è la tolleranza al singolo guasto. I requisiti stabiliscono come il sistema di sicurezza deve rispondere in presenza di "un singolo guasto", di "qualunque singolo guasto" o di "qualunque guasto di un singolo componente".

Riguardo ai guasti, devono essere considerati tre concetti molto importanti: (1) non tutti i guasti sono rilevati, (2) l'aggiunta della parola "componente" implica problematiche di cablaggio, (3) il cablaggio è parte integrante del sistema di sicurezza. I guasti di cablaggio possono provocare la perdita di una funzione di sicurezza.

L'intento dell'affidabilità del controllo è chiaramente l'operatività della funzione di sicurezza in presenza di un guasto. Se il guasto viene rilevato, il sistema di sicurezza deve eseguire una azione sicura, segnalare il guasto e impedire l'ulteriore funzionamento della macchina fino alla correzione del guasto. Se il guasto non viene rilevato, la funzione di sicurezza deve, su richiesta, poter essere ripetuta.

Introduzione alla sicurezza funzionale dei sistemi di controllo

IMPORTANTE: *gli standard e i requisiti considerati in questa sezione sono relativamente nuovi. Il lavoro è ancora in corso su alcuni aspetti, soprattutto per quanto riguarda il chiarimento e la combinazione di alcuni di questi standard. Quindi, è probabile che ci saranno delle variazioni rispetto ad alcuni dei dettagli forniti. Per le ultime informazioni, consultare: http://www.ab.com/safety.*

Al momento della pubblicazione di questo documento, c'è una crescente consapevolezza delle implicazioni di una nuova generazione di standard che coprono la sicurezza funzionale dei dispositivi e dei sistemi di controllo legati alla sicurezza.

Che cos'è la sicurezza funzionale?

Per sicurezza funzionale si intende quella parte della sicurezza complessiva che dipende dal corretto funzionamento del processo o delle apparecchiature in risposta ai relativi ingressi. Il sito web IEC, per contribuire a chiarire il significato di sicurezza funzionale, fornisce il seguente esempio. "Per esempio, un dispositivo di protezione contro le sovratemperature che utilizza un sensore termico negli avvolgimenti di un motore elettrico per diseccitare il motore prima che possano surriscaldarsi è un esempio di sicurezza funzionale. Ma l'isolamento di un componente contro le alte temperature non è un esempio di sicurezza funzionale (anche se è sempre un esempio di sicurezza e potrebbe proteggere esattamente dallo stesso pericolo)." Come ulteriore esempio, confrontiamo una protezione meccanica e una protezione interbloccata. La protezione meccanica non è considerata "sicurezza funzionale" anche se può proteggere contro l'accesso allo stesso pericolo, come una porta interbloccata. La porta interbloccata, invece, è un esempio di sicurezza funzionale. Quando la protezione è aperta, l'interblocco funge da ingresso per il sistema che garantisce lo stato di sicurezza. Anche i dispositivi di protezione personale (DPP) vengono utilizzati come misura protettiva per contribuire ad aumentare la sicurezza del personale. Ma i DPP non sono considerati sistemi di sicurezza funzionale.

Il termine "sicurezza funzionale" è stato introdotto in IEC 61508:1998. Da allora, è stato talvolta associato solo ai sistemi di sicurezza programmabili. Ma si tratta di una idea sbagliata. La sicurezza funzionale copre un'ampia gamma di dispositivi che vengono usati per creare sistemi di sicurezza. Dispositivi come interblocchi, barriere fotoelettriche, relè di sicurezza, PLC di sicurezza, contattori di sicurezza e azionamenti di sicurezza sono intercollegati per formare un sistema di sicurezza che realizza una specifica funzione di sicurezza. Questa è sicurezza funzionale. Quindi, la sicurezza funzionale di un sistema di controllo elettrico è altamente inerente al controllo dei pericoli proveniente dalle parti mobili di una macchina.

Per la sicurezza funzionale, sono necessari due tipi di requisiti:

- la funzione di sicurezza e
- l'integrità della sicurezza.

Il processo di valutazione dei rischi svolge un ruolo chiave nello sviluppo dei requisiti di sicurezza funzionale. I requisiti della funzione di sicurezza (quello che la funzione fa) derivano dall'analisi dei pericoli. La valutazione dei rischi produce i requisiti di integrità della sicurezza (la probabilità che una funzione di sicurezza venga realizzata in modo soddisfacente).

Di seguito, vengono descritti tre dei più significativi standard di sicurezza funzionale dei sistemi di controllo per i macchinari.

1. **IEC/EN 61508** "Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza".

   Questo standard contiene i requisiti e le disposizioni applicabili alla progettazione di sistemi e sottosistemi, elettronici e programmabili, complessi. Lo standard è generico e quindi non è limitato al settore delle macchine.

2. **IEC/EN 62061** "Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza".

   Si tratta dell'implementazione specifica per le macchine di IEC/EN 61508. Fornisce requisiti applicabili alla progettazione, a livello di sistema, di tutti i tipi di sistemi di controllo elettrici legati alla sicurezza dei macchinari, oltre che alla progettazione di dispositivi o sottosistemi non complessi. I sottosistemi programmabili o complessi dovrebbero soddisfare IEC/EN 61508.

3. **EN ISO 13849-1:2008** "Sicurezza delle macchine – Componenti legati alla sicurezza dei sistemi di controllo".

   Mira a fornire un percorso di transizione della sicurezza funzionale dalle Categorie.

Gli standard di sicurezza funzionale rappresentano un significativo passo avanti rispetto a requisiti esistenti come controllo affidabile e il sistema di categorie ISO 13849-1:1999 (EN 954-1:1996). Le categorie non sono ancora scomparse, lo standard originale rimarrà valido fino al 2010 per fornire un periodo di transizione alla nuova versione revisionata. Questa nuova versione di ISO/EN 13849-1 usa il concetto di sicurezza funzionale e ha introdotto una nuova terminologia e nuovi requisiti. In questa sezione, ci riferiremo alla nuova versione come EN ISO 13849-1:2008.

L'interesse negli standard di sicurezza funzionale crescerà perché sono il futuro e promuovono la flessibilità e l'uso di nuove tecnologie per la sicurezza delle macchine.

IEC/EN 62061 e EN ISO 13849-1:2008

Sia IEC/EN 62061 che EN ISO 13849-1:2008 riguardano i sistemi di controllo elettrici correlati alla sicurezza. Verranno eventualmente combinati come due parti di uno standard con terminologia comune. Entrambi gli standard producono lo stesso risultato utilizzando, tuttavia, metodi diversi. Sono concepiti per offrire all'utente la possibilità di scegliere quello più adatto alla propria situazione. Un utente può decidere di usare uno qualunque dei due standard.

I risultati di entrambi gli standard sono livelli comparabili di integrità o prestazioni di sicurezza. Le metodologie di ogni standard presentano differenze a seconda degli utenti a cui sono destinate. Una restrizione per EN ISO 13849-1:2008 è data nella Tabella 1 della sua introduzione. Quando si utilizza tecnologia programmabile e complessa, il massimo PL da considerare è PLd.

La metodologia IEC/EN 62061 mira a permettere l'uso di complesse funzionalità di sicurezza da implementare attraverso precedenti architetture di sistema non convenzionali. La metodologia EN ISO 13849-1:2008 ha come scopo la definizione di un percorso più diretto e meno complicato per garantire funzionalità di sicurezza più convenzionali implementate da architetture di sistema convenzionali.

Ancora una volta, la differenza fondamentale tra questi due standard è l'applicabilità alle varie tecnologie. IEC/EN 62061 è limitato ai sistemi elettrici. EN ISO 13849-1:2008 può essere invece applicato ai sistemi pneumatici, idraulici, meccanici ed elettrici.

Le descrizioni che seguono rivelano le similitudini, nei valori e nella logica, tra gli standard. Naturalmente, si tratta solamente di brevi accenni. Entrambi gli standard coprono molto altro rispetto a quanto riportato qui ed è importante considerarne i testi completi.

La seguente tabella presenta un diagramma di flusso semplificato che aiuta il progettista del sistema di sicurezza a determinare quale di questi due standard usare. Ogni percorso condivide processi comuni: funzioni di sicurezza e valutazione dei rischi. I dati di progettazione del sistema (ad es. PFH, MTTF, DC, SFF) cambiano perché cambia il percorso da uno standard all'altro.

SIL e IEC/EN 62061

IEC/EN 62061 descrive sia la quantità di rischio da ridurre che la capacità di un sistema di controllo di ridurre quel rischio in termini di SIL (Safety Integrity Level). Sono 3 i SIL usati nel settore delle macchine, SIL 1 è il più basso e SIL 3 il più alto.

Maggiori rischi possono verificarsi in altri settori come l'industria di processo e, per questo motivo, IEC 61508 e lo standard specifico per il settore di processo IEC 61511 includono SIL 4. Un SIL si applica a una funzione di sicurezza. I sottosistemi che costituiscono il sistema che implementa la funzione di sicurezza devono avere una adeguata capacità SIL. Questo, talvolta, è riferito come SIL Claim Limit (SIL CL). Prima che possa essere correttamente applicato, è necessario un completo e dettagliato studio di IEC/EN 62061. Alcuni dei requisiti più comunemente applicabili dello standard possono essere riepilogati come segue:

PL e EN ISO 13849-1:2008

EN ISO 13849-1:2008 non userà il termine SIL; userà il termine PL (Performance Level). Per molti aspetti, PL può essere collegato a SIL. I livelli prestazionali sono 5, PLa è il più basso e PLe il più alto.

Confronto tra PL e SIL

Questa tabella mostra la relazione approssimata tra PL e SIL quando applicate a tipiche strutture di circuito ottenute con tecnologia elettromeccanica a bassa complessità

PL (livello prestazionale)	PFH_D (Probabilità di guasti pericolosi all'ora)	SIL (Livello di integrità della sicurezza)
A	$\geq 10^{-5}$ a $<10^{-4}$	Nessuna
B	$\geq 3 \times 10^{-6}$ a $<10^{-5}$	1
C	$\geq 10^{-6}$ a $<3 \times 10^{-6}$	1
D	$\geq 10^{-7}$ a $<10^{-6}$	2
E	$\geq 10^{-8}$ a $<10^{-7}$	3

Corrispondenza approssimata tra PL e SIL

IMPORTANTE: *la tabella sopra riportata è soltanto indicativa e NON deve essere usata a scopi di conversione. Prendere in considerazione i requisiti completi degli standard.*

Progettazione del sistema secondo IEC/EN 62061

IEC/EN 62061, “Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza” è l’implementazione specifica per i macchinari di IEC/EN 61508. Fornisce requisiti applicabili alla progettazione, a livello di sistema, di tutti i tipi di sistemi di controllo elettrici legati alla sicurezza dei macchinari, oltre che alla progettazione di dispositivi o sottosistemi non complessi.

La valutazione dei rischi sfocia in una strategia di riduzione dei rischi che, a sua volta, identifica le esigenze relative alle funzioni di controllo di sicurezza. Queste funzioni devono essere documentate e devono includere quanto segue:

- specifica dei requisiti funzionali e
- specifica dei requisiti di integrità della sicurezza.

I requisiti funzionali sono dati quali frequenza di funzionamento, tempo di risposta richiesto, modalità operative, cicli di carico, ambiente operativo e funzioni di reazione ai guasti. I requisiti di integrità della sicurezza sono espressi in livelli di integrità della sicurezza (SIL). In base alla complessità del sistema, occorre considerare alcuni o tutti gli elementi nella tabella che segue, per determinare se la progettazione del sistema risponde ai SIL richiesti.

Elemento per la considerazione SIL	**Simbolo**
Probabilità di guasti pericolosi all’ora	PFH_D
Tolleranza ai guasti hardware	HFT
Percentuale di guasti sicuri	SFF
Intervallo tra test funzionali	T1
Intervallo tra test diagnostici	T2
Suscettibilità ai guasti per causa comune	ß
Copertura diagnostica	DC

Elementi per la considerazione dei SIL

Per i sistemi elettronici, un significativo contributo al guasto è il tempo, in relazione al numero di operazioni dei dispositivi elettromeccanici. Quindi, il tasso di guasto dei sistemi elettronici è su base oraria. Per determinare la loro probabilità di guasto, occorre intraprendere una analisi dei componenti. I sistemi di sicurezza sono specificamente interessati non solo alla probabilità di guasto ma anche, e in modo ancora più importante, alla probabilità di guasto pericoloso su base oraria, il PFHD. Una volta conosciuto questo dato, è possibile utilizzare la seguente tabella per determinare il SIL ottenuto.

SIL (Livello di integrità della sicurezza)	PFH_D (Probabilità di guasti pericolosi all'ora)
3	$\geq 10^{-8}$ a $< 10^{-7}$
2	$\geq 10^{-7}$ a $< 10^{-6}$
1	$\geq 10^{-6}$ a $< 10^{-5}$

Probabilità di guasto pericoloso per SIL

Il sistema di sicurezza è diviso in sottosistemi. Il livello di integrità di sicurezza hardware che può essere richiesto per un sottosistema è limitato dalla tolleranza ai guasti hardware e dalla percentuale di guasti sicuri dei sottosistemi. La tolleranza ai guasti hardware è la capacità del sistema di eseguire la sua funzione in presenza di guasti. Una tolleranza ai guasti di zero significa che la funzione non viene realizzata quando si verifica un singolo guasto. Una tolleranza ai guasti di uno permette al sottosistema di realizzare la sua funzione in presenza di un singolo guasto. La percentuale di guasti sicuri è la porzione del tasso di guasto globale che non comporta un guasto pericoloso. La combinazione di questi due elementi determina i vincoli hardware ed è denominata SILCL. La tabella che segue mostra la relazione tra vincoli hardware e SILCL.

SFF (percentuale di guasti sicuri)	Tolleranza ai guasti hardware		
	0	1	2
<60%	Non ammesso se non per specifiche eccezioni	SIL1	SIL2
60% – <90%	SIL1	SIL2	SIL3
90% – <99%	SIL2	SIL3	SIL3
≥99%	SIL3	SIL3	SIL3

Vincoli hardware su SIL

Per esempio, una architettura con tolleranza a un singolo guasto e una percentuale di guasti sicuri del 75% non può andare oltre SIL2, a prescindere dalla probabilità di guasto pericoloso.

Per calcolare la probabilità di guasto pericoloso, ogni funzione di sicurezza deve essere suddivisa in blocchi funzione, che vengono poi realizzati come sottosistemi. La progettazione del sistema di molte funzioni di sicurezza prevede un dispositivo di rilevamento collegato a un dispositivo logico collegato, a sua volta, a un attuatore. Questo crea una configurazione in serie di sottosistemi. Se possiamo determinare la probabilità di guasto pericoloso per ogni sottosistema e conoscere il suo SILCL, sarà possibile calcolare facilmente la probabilità di guasto del sistema sommando le probabilità di guasto dei sottosistemi. Questo concetto è spiegato di seguito.

SOTTOSISTEMA 1 Rilevamento posizione	SOTTOSISTEMA 2 Soluzione logica	SOTTOSISTEMA 3 Commutazione uscita
Requisiti funzionali e di integrità IEC/EN 62061	Requisiti funzionali e di integrità IEC/EN 62061	Requisiti funzionali e di integrità IEC/EN 62061
Vincoli hardware SIL CL 2	Vincoli hardware SIL CL 2	Vincoli hardware SIL CL 2
$PFH_D = 1x10^{-7}$	$PFH_D = 1x10^{-7}$	$PFH_D = 1x10^{-7}$

$= PFH_D\,1 \quad + PFH_D\,2 \quad + PFH_D\,3$

$= 1x10^{-7} \quad + 1x10^{-7} \quad + 1x10^{-7}$

$= 3x10^{-7}$ ovvero adatto per SIL2

Se, per esempio, vogliamo ottenere SIL2, ogni sottosistema deve avere un SIL Claim Limit (SIL CL) di almeno SIL2 e la somma del PFHD per il sistema non deve superare il limite consentito nella precedente tabella ‘Probabilità di guasto pericoloso per SIL’.

Il termine “sottosistema” ha uno speciale significato in IEC/EN 62061. Si tratta della suddivisione di primo livello di un sistema in parti che, se in guasto, provocano un guasto della funzione di sicurezza. Quindi, se in un sistema vengono usati due interruttori ridondanti, nessun singolo interruttore è un sottosistema. Il sottosistema sarebbe rappresentato da entrambi gli interruttori e dall’eventuale funzione di diagnostica guasti associata, se disponibile.

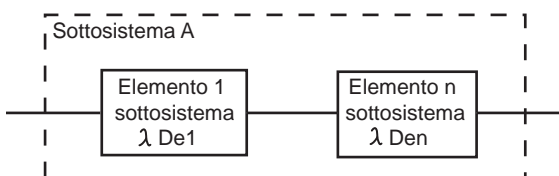
Progettazione del sottosistema – IEC/EN 62061

Se un progettista, nei sottosistemi, usa componenti “preconfezionati” conformi a IEC/EN 62061, tutto diventa più facile perché i requisiti specifici per la progettazione dei sottosistemi non si applicano. Questi requisiti saranno coperti, in generale, dal costruttore del dispositivo (sottosistema) e sono molto più complessi di quelli richiesti per la progettazione di sistema.

IEC/EN 62061 richiede che i sottosistemi complessi, come i PLC di sicurezza, siano conformi a IEC 61508. Ciò significa che, per dispositivi che usano componenti programmabili o elettronici complessi, IEC 61508 si applica in tutto il suo rigore. Questo può essere un processo molto difficile. Per esempio, la valutazione del PFH_D ottenuto da un sottosistema complesso può essere un processo molto complicato se si usano tecniche come la modellazione di Markov, gli schemi a blocchi per l’affidabilità o l’analisi dell’albero dei guasti.

IEC/EN 62061 non fornisce requisiti per la progettazione di sottosistemi di complessità inferiore. Generalmente, ciò includerebbe componenti elettrici relativamente semplici come interruttori interbloccati e relè di monitoraggio di sicurezza elettromeccanici. I requisiti non sono complessi come quelli in IEC 61508 ma possono ancora essere molto complicati.

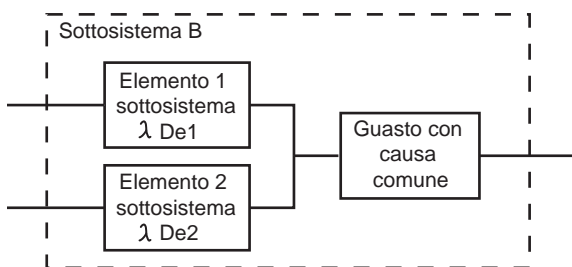
IEC/EN 62061 fornisce quattro architetture logiche dei sottosistemi, con relative formule, che possono essere usate per valutare il PFHD ottenuto da un sottosistema a bassa complessità. Queste architetture sono rappresentazioni puramente logiche e non dovrebbero essere pensate come architetture fisiche. Le quattro architetture logiche dei sottosistemi e relative formule sono riportate nei seguenti quattro schemi.

Per l'architettura dei sottosistemi di base mostrata di seguito, le probabilità di guasti pericolosi sono semplicemente sommate.

Architettura logica sottosistema A

$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$

$PFH_{DssA} = \lambda_{DssA} \times 1$ ora

λ, Lambda designa il tasso di guasto. Le unità del tasso di guasto sono guasti all'ora. λ_D, Lambda sub D è il tasso di guasto pericoloso. λ_{DssA}, Lambda sub DssA è il tasso di guasto pericoloso del sottosistema A. Lambda sub DssA è la somma dei tassi di guasto dei singoli elementi, e1, e2, e3, fino a en compreso. La probabilità di guasto pericoloso è moltiplicata per 1 ora, per creare la probabilità di guasto in un'ora.

Il diagramma successivo mostra un sistema tollerante a un singolo guasto, senza una funzione di diagnostica. Quando una architettura include la tolleranza a un singolo guasto, il potenziale dei guasti per causa comune esiste e deve essere considerato. La determinazione dei guasti per causa comune è brevemente descritta più avanti, in questo capitolo.

Architettura logica sottosistema B

$\lambda_{DssB} = (1-ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssB} = \lambda_{DssB} \times 1$ ora

Le formule per questa architettura prendono in considerazione la configurazione parallela degli elementi del sottosistema e aggiungono i seguenti due elementi dalla precedente tabella 'Elementi per la considerazione dei SIL'.

ß – la suscettibilità a guasti per causa comune (Beta)

T1 – l'intervallo tra test funzionali o ciclo di vita, a seconda di qual è il più breve. Il test funzionale è concepito per rilevare i guasti e il degrado del sottosistema di sicurezza, in modo che il sottosistema possa essere riportato a una condizione operativa.

Come esempio, ipotizziamo i seguenti valori:

ß = 0,10
$\lambda_{De1} = 1 \times 10^{-6}$ guasti/ora
$\lambda_{De2} = 1 \times 10^{-6}$ guasti/ora
T1 = 87600 ore (10 anni)

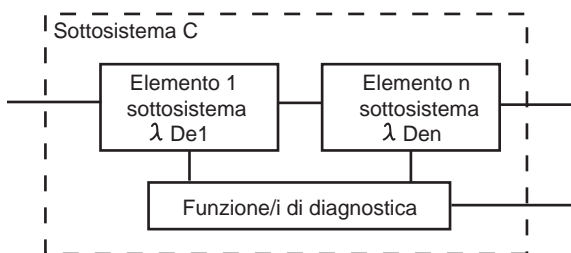
Il tasso di guasto per il sistema è 1.70956E-07 guasti all'ora (SIL2).

Influenza dell'intervallo tra test funzionali

Consideriamo l'influenza che ha sul sistema l'intervallo tra test funzionali. Presumiamo che l'intervallo tra test funzionali sia stato ridotto a due volte all'anno. Ciò riduce T1 a 4380 ore e il tasso di guasto pericoloso aumenta a 1.03548E-07 guasti all'ora. Questo è ancora solo SIL2. Se l'intervallo tra test funzionali diventa mensile (730 ore), il tasso di guasto pericoloso migliora a 1.0059E-07 guasti all'ora. Questo è ancora solo SIL2. Per raggiungere SIL3, è necessario un ulteriore miglioramento del tasso di guasto, dell'intervallo tra test funzionali o dei guasti per causa comune. Inoltre, il progettista deve tenere a mente che, per calcolare il tasso di guasto pericoloso globale, questo sottosistema deve essere combinato con altri sottosistemi.

Influenza dell'analisi dei guasti per causa comune

Guardiamo l'influenza che i guasti per causa comune hanno sul sistema. Supponiamo di adottare misure addizionali e di portare il nostro valore beta al suo miglior livello di 1% (0,01), mentre l'intervallo tra test funzionali rimane a 10 anni. Il tasso di guasto pericoloso aumenta a 9.58568E-08. Il sistema, adesso, arriva a SIL3.

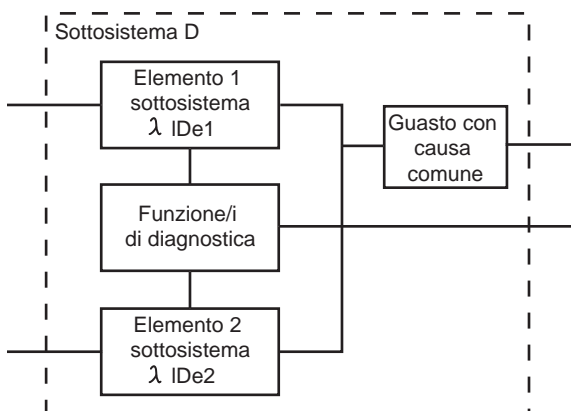
Il prossimo schema mostra la rappresentazione funzionale di un sistema a tolleranza zero, con una funzione diagnostica. La copertura diagnostica serve a ridurre la probabilità di guasti hardware pericolosi. I test diagnostici vengono realizzati automaticamente. La copertura diagnostica è il rapporto del tasso di guasti pericolosi rilevati rispetto al tasso di tutti i guasti pericolosi. Il tipo o il numero di guasti in sicurezza non è considerato quando si calcola la copertura diagnostica; si tratta solo della percentuale di guasti pericolosi rilevati.

Architettura logica sottosistema C

$$\lambda_{DssC} = \lambda_{De1} (1\text{-}DC_1) + \ldots + \lambda_{Den} (1\text{-}DC_n)$$
$$PFH_{DssC} = \lambda_{DssC} \times 1 \text{ ora}$$

Queste formule includono la copertura diagnostica (DC) per ogni elemento del sottosistema. I tassi di guasto di ognuno dei sottosistemi sono ridotti dalla copertura diagnostica di ogni sottosistema.

Di seguito, è riportato il quarto esempio di architettura di un sottosistema. Questo sottosistema è a tolleranza di un singolo guasto e include una funzione diagnostica. Con i sistemi a tolleranza di un singolo guasto, deve essere considerato anche il potenziale di guasti per causa comune.

Se gli elementi del sottosistema sono gli stessi, si usano le seguenti formule:

$$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De}^2 \times 2 \times DC \times T_2/2 + \lambda_{De}^2 \times (1\text{-}DC) \times T_1 \} + ß \times \lambda_{De}$$
$$PFH_{DssD} = \lambda_{DssD} \times 1 \text{ ora}$$

Architettura logica sottosistema D

Se gli elementi del sottosistema sono diversi, si usano le seguenti formule:

$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2/2 + \lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \times T_1/2 \} + ß \times (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssD} = \lambda_{DssD} \times 1$ ora

Notare che entrambe le formule usano un parametro addizionale, T2 ovvero l'intervallo di diagnostica.

Presumiamo i seguenti valori per l'esempio in cui gli elementi del sottosistema sono differenti:

- ß = 0,10
- λ_{De1} = 1 x 10 -6 guasti/ora
- λ_{De2} = 2 x 10 -6 guasti/ora
- T1 = 87.600 ore (10 anni)
- T2 = 876 ore
- DC1 = 0,8
- DC2 = 0,6

PFH_{DssD} = 2.36141E-07 guasti pericolosi/ora

Metodologia di transizione per le Categorie

Durante la redazione di IEC/EN 62061, il comitato ha preso atto che ci sarebbe voluto molto tempo perché tutti i dati richiesti, per sistemi e dispositivi, diventassero completamente disponibili. Per aiutare a convertire gli esistenti progetti di sottosistema, basati sul concetto delle categorie originali e già comprovati efficaci, sono state predisposte due tabelle. Forniscono l'equivalenza per PFH_D e vincoli hardware. Le tabelle favoriscono un utile percorso di transizione agli standard di sicurezza funzionali. In questo documento, sono state leggermente semplificate. Se analizzate, risulta evidente che le architetture di molti sistemi a categorie esemplificati nei precedenti capitoli possono essere considerate anche facendo riferimento agli standard di sicurezza funzionale.

Categoria	Tolleranza ai guasti	Copertura diagnostica	PFH_D che può essere richiesto per il sottosistema
1	0	0%	Vedere IEC/EN 62061
2	0	60% – 90%	$\geq 10^{-6}$
3	1	60% – 90%	$\geq 2 \times 10^{-7}$
4	>1	60% – 90%	$\geq 3 \times 10^{-8}$
	1	>90%	$\geq 3 \times 10^{-8}$

Richiesta PFHD per categoria

La precedente tabella 'Vincoli hardware su SIL' è una versione semplificata della Tabella 7 dello standard. Utilizzare questa tabella quando un sottosistema a categorie diventa parte di un SRCS che deve rispondere a IEC/EN 62061. Per semplicità, il progettista del sistema di sicurezza può chiedere un PFH_D di 2×10^{-7} per un sistema di categoria 3 con una copertura diagnostica del 60%. In alternativa, il progettista del sistema di sicurezza può effettuare una completa analisi per determinare se è possibile arrivare a un PFHD migliore.

Categoria	Tolleranza ai guasti	SFF	Massimo "SIL claim limit" in base ai vincoli hardware
1	0	<60%	Vedere IEC/EN 62061
2	0	60% – 90%	SIL1
3	1	<60%	SIL1
	1	60% – 90%	SIL2
4	>1	60% – 90%	SIL3

Vincoli hardware per categoria

La tabella ‘Richiesta PFHD per categoria’ può essere usata per determinare il SIL Claim Limit ovvero il SIL massimo di un sottosistema a categorie. La copertura diagnostica del sistema a categorie deve essere convertita in percentuale di guasti sicuri.

Conoscendo il PFH_D e il SIL CL di un sistema a categorie, il progettista del sistema di sicurezza può applicare questi valori in uno dei sottosistemi precedentemente mostrati. Se il sistema a categorie è l’SRCS completo, il SIL e il PFH_D equivalenti sono determinati dalle Tabelle ‘Vincoli hardware su SIL’ e ‘Richiesta PFHD per categorie’. Il progettista del sistema di sicurezza deve anche soddisfare i requisiti di guasti per causa comune, guasti sistematici e intervallo tra test funzionali. Il sistema di punteggio dei guasti per causa comune è leggermente diverso per ogni standard. I concetti per l’integrità della sicurezza sistematica sono simili in entrambi gli standard; nessuno standard usa un sistema di punteggio. L’intervallo tra test funzionali può essere considerato uguale al ciclo di vita o può essere stabilito un intervallo più corto.

Vincoli hardware

Il livello di integrità della sicurezza che può essere raggiunto, per un sistema o sottosistema, è limitato dalle caratteristiche dell’architettura. Le due principali caratteristiche sono la tolleranza ai guasti hardware e la percentuale di guasti sicuri. Tra le caratteristiche secondarie ci sono i guasti per causa comune e l’esclusione dei guasti.

Quando si combinano i sottosistemi, il SIL ottenuto dall’SRCS deve essere inferiore o uguale al SIL Claim Limit più basso tra i sottosistemi coinvolti nella funzione di controllo legata alla sicurezza.

B10 e $B10_d$

Per i sottosistemi elettromeccanici, la probabilità di guasto dovrebbe essere stimata prendendo in considerazione il numero di cicli operativi dichiarati dal costruttore, il carico e il ciclo di carico. La probabilità di guasto è espressa come il valore di B10, che è il tempo previsto a cui il 10% della popolazione genera un guasto. $B10_d$ è il tempo previsto a cui il 10% della popolazione genera un guasto pericoloso.

Guasti per causa comune (CCF)

I guasti per causa comune si verificano quando molteplici guasti, risultanti da una singola causa, producono un guasto pericoloso. Le informazioni sul CCF generalmente sono necessarie solo al progettista del sottosistema, di solito il costruttore. Nelle formule fornite serve a stimare il PFHD di un sottosistema. Generalmente, non sarà necessario per la progettazione del sistema. L’allegato F di IEC/EN 62061 propone un semplice approccio per la stima di CCF. La tabella che segue mostra un riepilogo del sistema di punteggio.

N.	Misura contro CCF	Punteggio
1	Separazione/Segregazione	25
2	Diversità	38
3	Progettazione/Applicazione/Esperienza	2
4	Valutazione/Analisi	18
5	Competenza/Formazione	4
6	Ambiente	18

Punteggio delle misure contro i guasti per causa comune

Per adottare misure specifiche contro i CCF, vengono assegnati dei punti. Il punteggio viene poi sommato per determinare il fattore dei guasti per causa comune, mostrato nella seguente tabella. Il fattore beta serve a “regolare” il tasso di guasto nei modelli di sottosistema.

Punteggio totale	Fattore guasti per causa comune (ß)
<35	10% (0,1)
35 – 65	5% (0,05)
65 – 85	2% (0,02)
85 – 00	1% (0,01)

Fattore Beta per i guasti per causa comune

Copertura diagnostica (DC)

Per ridurre la probabilità di pericolosi guasti hardware, si utilizzano test di diagnostica automatica. Essendo in grado di rilevare il 100% dei guasti hardware pericolosi sarebbe ideale, ma è spesso molto difficile da ottenere.

La copertura diagnostica è il rapporto dei guasti pericolosi rilevati rispetto a tutti i guasti pericolosi.

$$DC = \frac{\text{Tasso di guasti pericolosi rilevati, } \lambda_{DD}}{\text{Tasso di guasti pericolosi totali, } \lambda_{Dtotal}}$$

Il valore di copertura diagnostica sarà tra zero e uno.

Tolleranza ai guasti hardware

La tolleranza ai guasti hardware rappresenta il numero di guasti che possono essere sostenuti da un sottosistema prima di generare un guasto pericoloso. Per esempio, una tolleranza ai guasti hardware di 1 significa che 2 guasti potrebbero provocare una perdita della funzione di controllo legata alla sicurezza, ma un solo guasto no.

Gestione della sicurezza funzionale

Lo standard fornisce i requisiti per il controllo delle attività tecniche e di gestione necessarie all'ottenimento di un sistema di controllo elettrico legato alla sicurezza.

Probabilità di guasto pericoloso (PFH_D)

Parte dei requisiti necessari per ottenere una determinata capacità SIL di un sistema o sotto-sistema è il PFH_D (probabilità di un guasto pericoloso all'ora) dovuto a guasti hardware casuali.

I dati saranno forniti dal costruttore. I dati per i recenti sistemi e componenti di sicurezza Rockwell Automation (ad es. GuardLogix, GuardPLC, SmartGuard e Kinetix con GuardMotion, interruttori di interblocco, pulsanti di emergenza, ecc.) sono già disponibili.

IEC/EN 62061 chiarisce anche che, se e dove applicabile, possono essere utilizzati i Reliability Data Handbook.

Per i dispositivi elettromeccanici a bassa complessità, il meccanismo di guasto è generalmente collegato al numero e alla frequenza delle operazioni anziché solo al tempo. Quindi, per questi componenti, i dati deriveranno da qualche test sul ciclo di vita (ad es. B10). B10 è il numero di operazioni. Una serie di informazioni legate all'applicazione, come il numero previsto di opera-zioni all'anno, è poi necessaria per convertire $B10_d$ o simili dati in $MTTF_d$ (tempo medio prima di un guasto pericoloso). Questo viene, a sua volta, convertito in PFH_D.

In generale, si può ipotizzare quanto segue:

$$PFH_D = 1/MTTF_d$$

E per i dispositivi elettromeccanici:

$$MTTF_d = B_{10d}/(0,1 \times \text{numero medio di operazioni all'anno})$$

La formula di $MTTF_d$ è basata sul presupposto di un tasso di guasto costante. La distribuzione cumulativa dei guasti è $F(t) = 1 - \exp(-\lambda_d t)$.

Intervallo tra i test funzionali

L'intervallo tra i test funzionali rappresenta il tempo dopo cui un sottosistema deve essere totalmente controllato o sostituito per garantire che sia "come nuovo". In pratica, nel settore delle macchine, ciò si ottiene mediante sostituzione. Quindi, l'intervallo tra i test funzionali corrisponde, di solito, al ciclo di vita. EN ISO 13849-1:2008 fa riferimento a questo come ciclo di vita.

Un test funzionale è un controllo che può rilevare i guasti e l'usura di un SRCS in modo da poterlo riportare, per quanto possibile, in condizioni di "come nuovo". Il test funzionale deve rilevare il 100% di tutti i guasti pericolosi. Canali separati devono essere testati separatamente.

Diversamente dai test diagnostici, che sono automatici, i test funzionali vengono generalmente realizzati manualmente e offline. Essendo automatici, i test diagnostici sono realizzati più spesso rispetto ai test funzionali che, invece, vengono realizzati raramente. Per esempio, i circuiti collegati all'interruttore di interblocco di una protezione possono essere testati automaticamente, per cortocircuiti o interruzioni, con i test diagnostici (ad es. a impulsi).

L'intervallo tra i test funzionali deve essere dichiarato dal costruttore. Talvolta, il costruttore fornisce una serie di intervalli tra test funzionali differenti. L'intervallo tra test funzionali più adeguato è determinato esaminando le formule per l'architettura selezionata. In generale, più breve è l'intervallo tra i test funzionali, minore sarà il tasso di guasto.

SFF (percentuale di guasti sicuri)

La percentuale di guasti sicuri è simile alla copertura diagnostica ma considera anche qualunque tendenza intrinseca a generare un guasto in stato di sicurezza. Per esempio, un fusibile bruciato è un guasto ma è altamente probabile che si risolva in una interruzione di circuito che, in molti casi, è un guasto "sicuro". SFF (la somma del tasso di guasti "sicuri" più il tasso di guasti pericolosi rilevati) viene diviso per (la somma del tasso di guasti "sicuri" più il tasso di guasti pericolosi rivelati e non rivelati). È importante capire che i soli tipi di guasto da considerare sono quelli che potrebbero avere qualche effetto sulla funzione di sicurezza.

Molti dispositivi meccanici a bassa complessità – come pulsanti di emergenza e interruttori di interblocco – avranno (da soli) un SFF inferiore al 60% ma molti dispositivi elettronici di sicurezza sono concepiti con ridondanza e monitoraggio e quindi è facile che il valore SFF superi il 90%. Il valore SFF viene generalmente fornito dal costruttore.

Il valore SFF può essere calcolato con la seguente equazione:

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$$

dove:

λ_S = tasso di guasti sicuri,
$\Sigma\lambda_S + \Sigma\lambda_D$ = tasso di guasti totale,
λ_{DD} = tasso di guasti pericolosi rilevati
λ_D = tasso di guasti pericolosi.

Guasti sistematici

Lo standard ha requisiti per il controllo e l'eliminazione dei guasti sistematici. I guasti sistematici sono diversi dai guasti hardware casuali che si verificano, di solito, per usura dei componenti hardware. Possibili guasti sistematici sono errori di progettazione software, errori di progettazione hardware, errori di specifica dei requisiti e procedure operative. Tra le misure necessarie a evitare i guasti sistematici ci sono le seguenti:

- corretta selezione, combinazione, disposizione, assemblaggio e installazione dei componenti;
- uso di buone pratiche di progettazione;
- rispetto delle specifiche del costruttore e delle istruzioni di installazione;
- verifica della compatibilità tra i componenti;
- compatibilità alle condizioni ambientali;
- uso di materiali adatti.

Lo standard fornisce requisiti aggiuntivi e più dettagliati per evitare i guasti sistematici. Lo standard non contiene un sistema di punteggio per determinare quale percentuale dei potenziali guasti sistematici è coperta. Per ottenere SIL3, il progettista deve soddisfare tutti i requisiti per evitare i guasti sistematici. Se non si rispettano tutti i requisiti, il SIL Claim Limit deve essere ridotto.

Progettazione dei sistemi conformemente a EN ISO 13849-1:2008

Prima che possa essere correttamente applicato, è necessario un completo e dettagliato studio di EN ISO 13849-1:2008. Quanto segue è una breve presentazione:

Questo standard fornisce i requisiti per la progettazione e l'integrazione dei componenti di sicurezza dei sistemi di controllo, compresi alcuni elementi software. Lo standard si applica a un sistema di sicurezza ma può anche applicarsi ai componenti del sistema. Questo standard, inoltre, è di ampia applicabilità, dato che vale per tutte le tecnologie (elettrica, idraulica, pneumatica, meccanica, ecc.). Sebbene ISO 13849-1 sia applicabile ai sistemi complessi, per i sistemi complessi con software integrato rimanda il lettore a IEC 62061 e IEC 61508.

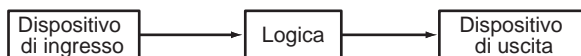
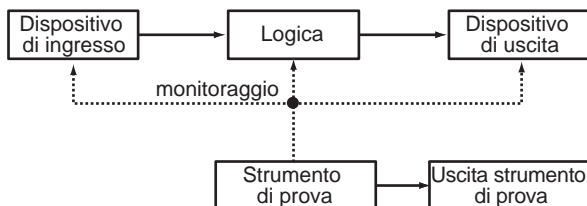
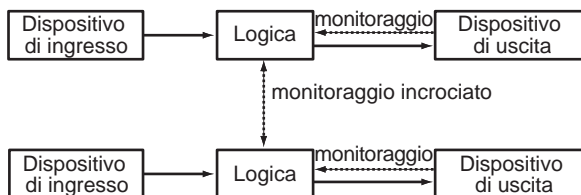
Con questo standard, l'integrità della sicurezza di un sistema è classificata in 5 PL (livelli prestazionali). PLa è l'integrità più bassa e PLe quella più alta. Vengono valutati considerando i seguenti fattori:

Struttura (architettura). Questi fattori sono direttamente correlati alle categorie, come spiegato precedentemente in questo documento.

Ciclo di vita – vita operativa prevista
MTTFd – tempo medio prima di un guasto pericoloso
DC – copertura diagnostica
CCF – guasti per causa comune
Comportamento in condizioni di guasto
Software
Guasti sistematici
Condizioni ambientali

Architetture dei sistemi di sicurezza (strutture)

Per la stima del PL, lo standard fornisce una procedura semplificata a categorie. L'intenzione di questo approccio è fornire un riconoscibile percorso di transizione dallo standard a categorie originale alla versione 2006 basata sui livelli prestazionali. Lo standard fornisce 5 architetture designate, illustrate di seguito. Corrispondono alle attuali 5 Categorie B, 1, 2, 3 e 4. Questi diagrammi devono essere studiati con attenzione nella clausola 6 dello standard, dove sono spiegati i requisiti, le differenze e i presupposti. I diagrammi delle architetture per le Categorie B e 1 e anche per 3 e 4 possono sembrare uguali ma lo standard spiega le differenze di dettaglio in termini di requisiti, tra cui la copertura diagnostica, ecc.

Sarà anche utile studiare la spiegazione dettagliata delle categorie contenuta in questa pubblicazione che, inoltre, riporta esempi pratici per la loro implementazione. I tre diagrammi che seguono mostrano gli schemi a blocchi delle 5 architetture, come mostrate in ISO/EN 13849-1.

Architettura designata per le Categorie B e 1

Architettura designata per la Categoria 2

Architettura designata per le Categoria 3 e 4

Ciclo di vita

Il ciclo di vita rappresenta il massimo periodo di tempo per cui un sottosistema (o sistema) può essere usato. Al termine di questo periodo, deve essere sostituito. Il ciclo di vita deve essere dichiarato dal costruttore dei componenti. Il ciclo di vita è generalmente uguale all'intervallo tra test funzionali, definito in IEC/EN 62061. Il progettista del sistema di sicurezza deve quindi considerare il ciclo di vita dei componenti per determinare il ciclo di vita di ogni funzione di sicurezza.

Tempo medio prima di un guasto pericoloso ($MTTF_d$)

$MTTF_d$ (tempo medio prima di un guasto pericoloso) è usato direttamente in EN ISO 13849-1:2008 per la stima del PL. Lo standard propone tre metodi per determinare $MTTF_d$: 1) uso dei dati del costruttore, 2) uso degli Allegati C e D che forniscono i tassi di guasto dei componenti, 3) uso di un valore di default di 10 anni. La selezione del valore di default restringe il campo a Medio, come mostrato nella tabella che segue.

Denotazione MTTFd di ogni canale	**Campo MTTFd di ogni canale**
Basso	3 anni <= MTTFd <10 anni
Medio	10 anni <= MTTFd <30 anni
Alto	30 anni <= MTTFd <100 anni

Livelli di $MTTF_d$

Quando il sistema di sicurezza prevede l'interfaccia con IEC 62061, il numero $MTTF_d$ deve essere convertito in PFH_D. Ciò avviene usando la seguente relazione:

$$PFH_D = 1/MTTF_d$$

E per i dispositivi elettromeccanici:

$$MTTF_d = B10_d/(0,1 \text{ x numero medio di operazioni all'anno})$$

In molti casi, è richiesto anche per la determinazione del PFH_D. Viene fornito dai costruttori. $MTTF_d$ e PFH_D deriveranno, generalmente, dallo stesso tipo di test o dagli stessi dati di analisi. Per i dispositivi elettromeccanici a bassa complessità, il meccanismo di guasto è generalmente collegato al numero e alla frequenza delle operazioni anziché solo al tempo. Quindi, per questi componenti, i dati deriveranno da qualche forma di test sul ciclo di vita (ad es. B10). Una serie di informazioni legate all'applicazione, come il numero previsto di operazioni all'anno, è poi necessaria per convertire $B10_d$ o dati simili in $MTTF_d$.

Copertura diagnostica (DC)

La copertura diagnostica (DC) rappresenta l'efficacia del monitoraggio dei guasti di un sistema o sottosistema. DC è il rapporto tra il tasso di guasti pericolosi rilevati e il tasso totale dei guasti pericolosi. EN ISO 13849-1:2008 e IEC 61508 forniscono delle tabelle che possono essere usate per ricavare DC e, in alcuni casi, questo valore può essere fornito dai costruttori.

Guasti per causa comune (CCF)

I guasti per causa comune (CCF) si verificano quando molteplici guasti, risultanti da una singola causa, producono un guasto pericoloso. Si tratta di guasti di diversi elementi, derivanti da un singolo evento. I guasti non sono conseguenti uno all'altro. L'Allegato F di EN ISO 13849-1:2008 fornisce un metodo qualitativo semplificato per determinare il CCF. La tabella che segue mostra un riepilogo del sistema di punteggio.

N.	Misura contro CCF	Punteggio
1	Separazione/Segregazione	15
2	Diversità	20
3	Progettazione/Applicazione/Esperienza	20
4	Valutazione/Analisi	5
5	Competenza/Formazione	5
6	Ambiente	35

Punteggio per i guasti per causa comune

Per la conformità alle Categorie 2, 3 e 4, occorre raggiungere un punteggio di almeno 65.

Guasti sistematici

Gli standard hanno requisiti per il controllo e l'eliminazione dei guasti sistematici. Possibili guasti sistematici sono errori di progettazione software, errori di progettazione hardware ed errori di specifica dei requisiti.

I guasti sistematici sono diversi dai guasti hardware casuali che si verificano, di solito, per usura dei componenti hardware. L'Allegato G di EN ISO 13849-1:2008 descrive le misure per il controllo e l'eliminazione dei guasti sistematici.

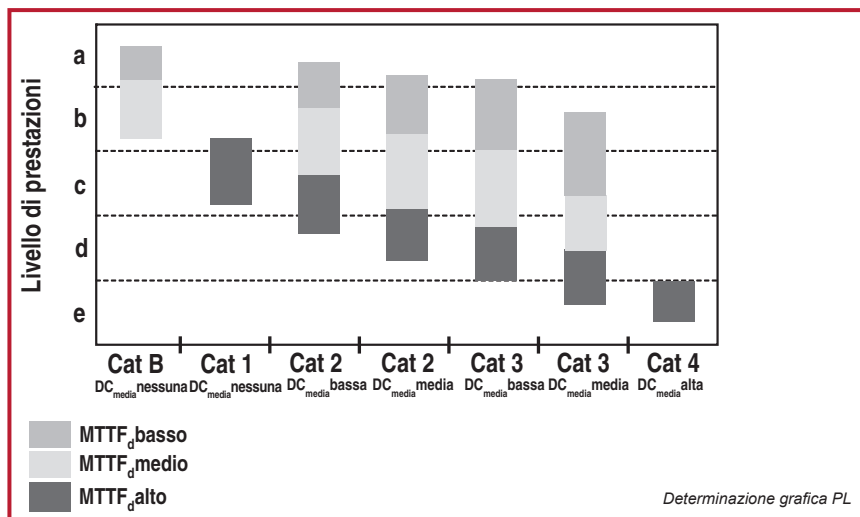
Livelli prestazionali (PL)

Quando si valutano i criteri progettuali nella precedente tabella 'Livelli di $MTTD_d$', agli SRCS verrà assegnato un livello prestazionale. Il livello prestazionale è un livello discreto che specifica la capacità dei componenti di sicurezza del sistema di controllo di realizzare una funzione di sicurezza.

Per valutare il PL ottenuto mediante l'implementazione di una delle 5 architetture, sono necessari i seguenti dati del sistema (o sottosistema):

- $MTTF_d$ (tempo medio prima di un guasto pericoloso di ogni canale)
- DC (copertura diagnostica)
- Architettura (la categoria)

Il seguente diagramma mostra un metodo grafico per determinare il PL dalla combinazione di questi fattori. La tabella alla fine di questa sezione mostra i risultati tabulari di differenti modelli Markov che sono alla base di questo diagramma. Quando è necessaria una determinazione più accurata, consultare la tabella.

Determinazione grafica PL

Come si può notare, ci sono delle sovrapposizioni nelle linee di divisione dei PL. Se MTTF è fornito solo in termini categorici (basso, medio, alto), usare il prossimo diagramma per determinare il PL.

Metodo grafico semplificato

Per esempio, una applicazione usa l'architettura di Categoria 3. Se DC è tra il 60% e il 90%, e se $MTTF_d$ di ogni canale è tra 10 e 30 anni, secondo la Figura 10.7, si ottiene PLd.

Per ottenere il PL necessario, devono essere realizzati anche altri fattori. Questi requisiti includono le disposizioni per i guasti per causa comune, i guasti sistematici, le condizioni ambientali e il ciclo di vita.

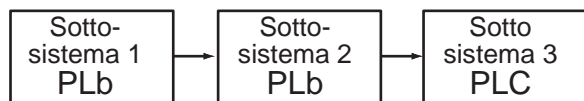
Se il PFH_D del sistema o sottosistema è conosciuto, la Tabella 10.4 (Allegato K dello standard) può essere usata per ricavare il PL.

Progettazione dei sottosistemi e combinazioni

I sottosistemi conformi a un PL possono essere combinati semplicemente in un sistema usando la Tabella 10.3. La logica dietro questa tabella è chiara. Primo, il sistema può essere affidabile solo quanto il più debole dei sottosistemi. Secondo, più sono i sottosistemi, maggiore è la possibilità di guasto.

PL_{basso}	N_{basso}	PL
a	>3	non ammesso
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

Calcolo del PL per sottosistemi combinati in serie

Nel sistema mostrato nel diagramma che segue, i livelli prestazionali più bassi sono quelli dei sottosistemi 1 e 2. Entrambi sono PLb. Quindi, usando questa tabella, possiamo seguire i dati b (nella colonna PL_{basso}) e 2 (nella colonna N_{basso}) per trovare il PL del sistema come b (nella colonna PL). Se tutti e tre i sottosistemi fossero stati PLb, il PL risultante sarebbe stato PLa.

Combinazione di sottosistemi in serie come sistema PLb

Convalida

La convalida svolge un ruolo importante in tutto il processo di sviluppo e di messa in servizio del sistema di sicurezza. ISO/EN 13849-2:2003 stabilisce i requisiti per la convalida dei sistemi concepiti conformemente all'originale ISO 13849-1 (EN 954-1). Si sa che questo standard sarà revisionato per allinearlo a EN ISO 13849-1:2008. In ISO 13849-2, la convalida impone un piano di convalida e la discussione mediante tecniche di analisi e di prova quali l'analisi dell'albero dei guasti e dei modi, degli effetti e della criticità dei guasti. Molti di questi requisiti si applicheranno al costruttore del sottosistema anziché all'utilizzatore.

Messa in servizio delle macchine

In fase di messa in servizio delle macchine o del sistema, deve essere effettuata una convalida delle funzioni di sicurezza, in tutte le modalità operative, che dovrebbe coprire tutte le condizioni anomale prevedibili e normali. Anche le combinazioni di ingressi e sequenze di funzionamento dovrebbero essere considerate. Questa procedura è importante perché è sempre necessario controllare che il sistema sia adatto alle caratteristiche ambientali e operative esistenti.

Alcune di queste caratteristiche possono essere diverse da quelle anticipate in fase progettuale.

Esclusione dei guasti

Uno dei principali strumenti di analisi per i sistemi di sicurezza è l'analisi dei guasti. Il progettista e l'utilizzatore devono capire come funziona il sistema di sicurezza in presenza di guasti. Sono molte le tecniche disponibili per realizzare questa analisi. Per esempio, analisi dell'albero dei guasti; analisi dei modi, degli effetti e della criticità dei guasti; analisi dell'albero degli eventi; analisi "load-strength".

Durante l'analisi, possono rimanere scoperti alcuni guasti impossibili da rilevare con la diagnostica automatica, se non con alti costi economici. Inoltre, la probabilità che tali guasti si verifichino può essere molto ridotta usando appositi metodi di progettazione, costruzione e verifica. In queste condizioni, i guasti possono essere esclusi da ulteriore considerazione. L'esclusione dei guasti è la mancata considerazione di un guasto vista la scarsa probabilità che si verifichi quel guasto specifico dell'SRCS.

EN ISO 13849-1:2008 ammette l'esclusione dei guasti in base all'improbabilità tecnica che si verifichino, all'esperienza tecnica comune e ai requisiti tecnici legati all'applicazione. ISO 13849-2:2003 fornisce una serie di esempi e giustificazioni per escludere certi guasti per i sistemi elettrici, pneumatici, idraulici e meccanici. L'esclusione dei guasti deve essere dichiarata con giustificazioni dettagliate, fornite nella documentazione tecnica.

L'esclusione dei guasti può portare a un PL molto alto. Durante tutto il ciclo di vita della macchina, occorre prevedere adeguate misure per permettere l'esclusione dei guasti. Non è sempre possibile valutare un SRCS senza presumere che certi guasti possano essere esclusi. Per informazioni dettagliate sull'esclusione dei guasti, vedere ISO 13849-2.

MTTFd per ogni canale in anni	Probabilità media di guasti pericolosi all'ora (1/h) e corrispondente livello prestazionale (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{media} = nessuna		DC_{media} = nessuna		DC_{media} = bassa		DC_{media} = media		DC_{media} = bassa		DC_{media} = media		DC_{media} = alta	
3	$3,80 \times 10^{-5}$	a			$2,58 \times 10^{-5}$	a	$1,99 \times 10^{-5}$	a	$1,26 \times 10^{-5}$	a	$6,09 \times 10^{-6}$	b		
3,3	$3,46 \times 10^{-5}$	a			$2,33 \times 10^{-5}$	a	$1,79 \times 10^{-5}$	a	$1,13 \times 10^{-5}$	a	$5,41 \times 10^{-6}$	b		
3,6	$3,17 \times 10^{-5}$	a			$2,13 \times 10^{-5}$	a	$1,62 \times 10^{-5}$	a	$1,03 \times 10^{-5}$	a	$4,86 \times 10^{-6}$	b		
3,9	$2,93 \times 10^{-5}$	a			$1,95 \times 10^{-5}$	a	$1,48 \times 10^{-5}$	a	$9,37 \times 10^{-6}$	b	$4,40 \times 10^{-6}$	b		
4,3	$2,65 \times 10^{-5}$	a			$1,76 \times 10^{-5}$	a	$1,33 \times 10^{-5}$	a	$8,39 \times 10^{-6}$	b	$3,89 \times 10^{-6}$	b		
4,7	$2,43 \times 10^{-5}$	a			$1,60 \times 10^{-5}$	a	$1,20 \times 10^{-5}$	a	$7,58 \times 10^{-6}$	b	$3,48 \times 10^{-6}$	b		
5,1	$2,24 \times 10^{-5}$	a			$1,47 \times 10^{-5}$	a	$1,10 \times 10^{-5}$	a	$6,91 \times 10^{-6}$	b	$3,15 \times 10^{-6}$	b		
5,6	$2,04 \times 10^{-5}$	a			$1,33 \times 10^{-5}$	a	$9,87 \times 10^{-6}$	b	$6,21 \times 10^{-6}$	b	$2,80 \times 10^{-6}$	c		
6,2	$1,84 \times 10^{-5}$	a			$1,19 \times 10^{-5}$	a	$8,80 \times 10^{-6}$	b	$5,53 \times 10^{-6}$	b	$2,47 \times 10^{-6}$	c		
6,8	$1,68 \times 10^{-5}$	a			$1,08 \times 10^{-5}$	a	$7,93 \times 10^{-6}$	b	$4,98 \times 10^{-6}$	b	$2,20 \times 10^{-6}$	c		
7,5	$1,52 \times 10^{-5}$	a			$9,75 \times 10^{-6}$	b	$7,10 \times 10^{-6}$	b	$4,45 \times 10^{-6}$	b	$1,95 \times 10^{-6}$	c		
8,2	$1,39 \times 10^{-5}$	a			$8,87 \times 10^{-6}$	b	$6,43 \times 10^{-6}$	b	$4,02 \times 10^{-6}$	b	$1,74 \times 10^{-6}$	c		
9,1	$1,25 \times 10^{-5}$	a			$7,94 \times 10^{-6}$	b	$5,71 \times 10^{-6}$	b	$3,57 \times 10^{-6}$	b	$1,53 \times 10^{-6}$	c		
10	$1,14 \times 10^{-5}$	a			$7,18 \times 10^{-6}$	b	$5,14 \times 10^{-6}$	b	$3,21 \times 10^{-6}$	b	$1,36 \times 10^{-6}$	c		
11	$1,04 \times 10^{-5}$	a			$6,44 \times 10^{-6}$	b	$4,53 \times 10^{-6}$	b	$2,81 \times 10^{-6}$	c	$1,18 \times 10^{-6}$	c		
12	$9,51 \times 10^{-5}$	b			$5,84 \times 10^{-6}$	b	$4,04 \times 10^{-6}$	b	$2,49 \times 10^{-6}$	c	$1,04 \times 10^{-6}$	c		
13	$8,78 \times 10^{-5}$	b			$5,33 \times 10^{-6}$	b	$3,64 \times 10^{-6}$	b	$2,23 \times 10^{-6}$	c	$9,21 \times 10^{-7}$	d		
15	$7,61 \times 10^{-6}$	b			$4,53 \times 10^{-6}$	b	$3,01 \times 10^{-6}$	b	$1,82 \times 10^{-6}$	c	$7,44 \times 10^{-7}$	d		
16	$7,31 \times 10^{-6}$	b			$4,21 \times 10^{-6}$	b	$2,77 \times 10^{-6}$	c	$1,67 \times 10^{-6}$	c	$6,76 \times 10^{-7}$	d		

MTTFd per ogni canale in anni	Probabilità media di guasti pericolosi all'ora (1/h) e corrispondente livello prestazionale (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{media} = nessuna		DC_{media} = nessuna		DC_{media} = bassa		DC_{media} = media		DC_{media} = bassa		DC_{media} = media		DC_{media} = alta	
18	$6,34 \times 10^{-6}$	b			$3,68 \times 10^{-6}$	b	$2,37 \times 10^{-6}$	c	$1,41 \times 10^{-6}$	c	$5,67 \times 10^{-7}$	d		
20	$5,71 \times 10^{-6}$	b			$3,26 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,22 \times 10^{-6}$	c	$4,85 \times 10^{-7}$	d		
22	$5,19 \times 10^{-6}$	b			$2,93 \times 10^{-6}$	c	$1,82 \times 10^{-6}$	c	$1,07 \times 10^{-6}$	c	$4,21 \times 10^{-7}$	d		
24	$4,76 \times 10^{-6}$	b			$2,65 \times 10^{-6}$	c	$1,62 \times 10^{-6}$	c	$9,47 \times 10^{-7}$	d	$3,70 \times 10^{-7}$	d		
27	$4,23 \times 10^{-6}$	b			$2,32 \times 10^{-6}$	c	$1,39 \times 10^{-6}$	c	$8,04 \times 10^{-7}$	d	$3,10 \times 10^{-7}$	d		
30			$3,80 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,21 \times 10^{-6}$	c	$6,94 \times 10^{-7}$	d	$2,65 \times 10^{-7}$	d	$9,54 \times 10^{-8}$	e
33			$3,46 \times 10^{-6}$	b	$1,85 \times 10^{-6}$	c	$1,06 \times 10^{-6}$	c	$5,94 \times 10^{-7}$	d	$2,30 \times 10^{-7}$	d	$8,57 \times 10^{-8}$	e
36			$3,17 \times 10^{-6}$	b	$1,67 \times 10^{-6}$	c	$9,39 \times 10^{-7}$	d	$5,16 \times 10^{-7}$	d	$2,01 \times 10^{-7}$	d	$7,77 \times 10^{-8}$	e
39			$2,93 \times 10^{-6}$	c	$1,53 \times 10^{-6}$	c	$8,40 \times 10^{-7}$	d	$4,53 \times 10^{-7}$	d	$1,78 \times 10^{-7}$	d	$7,11 \times 10^{-8}$	e
43			$2,65 \times 10^{-6}$	c	$1,37 \times 10^{-6}$	c	$7,34 \times 10^{-7}$	d	$3,87 \times 10^{-7}$	d	$1,54 \times 10^{-7}$	d	$6,37 \times 10^{-8}$	e
47			$2,43 \times 10^{-6}$	c	$1,24 \times 10^{-6}$	c	$6,49 \times 10^{-7}$	d	$3,35 \times 10^{-7}$	d	$1,34 \times 10^{-7}$	d	$5,76 \times 10^{-8}$	e
51			$2,24 \times 10^{-6}$	c	$1,13 \times 10^{-6}$	c	$5,80 \times 10^{-7}$	d	$2,93 \times 10^{-7}$	d	$1,19 \times 10^{-7}$	d	$5,26 \times 10^{-8}$	e
56			$2,04 \times 10^{-6}$	c	$1,02 \times 10^{-6}$	c	$5,10 \times 10^{-7}$	d	$2,52 \times 10^{-7}$	d	$1,03 \times 10^{-7}$	d	$4,73 \times 10^{-8}$	e
62			$1,84 \times 10^{-6}$	c	$9,06 \times 10^{-7}$	d	$4,43 \times 10^{-7}$	d	$2,13 \times 10^{-7}$	d	$8,84 \times 10^{-8}$	e	$4,22 \times 10^{-8}$	e
68			$1,68 \times 10^{-6}$	c	$8,17 \times 10^{-7}$	d	$3,90 \times 10^{-7}$	d	$1,84 \times 10^{-7}$	d	$7,68 \times 10^{-8}$	e	$3,80 \times 10^{-8}$	e
75			$1,52 \times 10^{-6}$	c	$7,31 \times 10^{-7}$	d	$3,40 \times 10^{-7}$	d	$1,57 \times 10^{-7}$	d	$6,62 \times 10^{-8}$	e	$3,41 \times 10^{-8}$	e
82			$1,39 \times 10^{-6}$	c	$6,61 \times 10^{-7}$	d	$3,01 \times 10^{-7}$	d	$1,35 \times 10^{-7}$	d	$5,79 \times 10^{-8}$	e	$3,08 \times 10^{-8}$	e
91			$1,25 \times 10^{-6}$	c	$5,88 \times 10^{-7}$	d	$2,61 \times 10^{-7}$	d	$1,14 \times 10^{-7}$	d	$4,94 \times 10^{-8}$	e	$2,74 \times 10^{-8}$	e
100			$1,14 \times 10^{-6}$	c	$5,28 \times 10^{-7}$	d	$2,29 \times 10^{-7}$	d	$1,01 \times 10^{-7}$	d	$4,29 \times 10^{-8}$	e	$2,47 \times 10^{-8}$	e